NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USING SURVEILLANCE CAMERA SYSTEMS TO MONITOR PUBLIC DOMAINS: CAN ABUSE BE PREVENTED?

by

Thomas J. Nestel, III

March 2006

Thesis Advisor:	David Brannan
Second Reader:	Jerry Ratcliffe

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503..			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse Be Prevented?			**5. FUNDING NUMBERS**
6. AUTHOR(S) Thomas J. Nestel, III			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

After mainland United States suffered a violent attack upon its citizenry, Homeland Security professionals recognized the need to protect a growing number of critical infrastructure locations. Millions of dollars earmarked for emergency management programs were funneled into technologies that enabled public safety to "do more with less." Closed circuit television surveillance systems rocketed to the forefront as the must-have technology. Citizens of the United States became subject to video surveillance during their normal daily routines.

This thesis examines the management of CCTV systems used by municipal police departments and analyzes the policies created to control the technology and prevent abuse. Using U.S. Census Bureau data, the police departments responsible for protecting the 50 largest cities were contacted and surveyed. The initial step determined what jurisdictions utilized surveillance cameras to monitor public domains. The follow-up steps gathered information about the systems being used; the management decisions regarding where to place the cameras; the training for its operators; supervision standards; the written policies regulating the department's program; analyzing those directives; and finally, presenting step-by-step recommendations for implementing CCTV surveillance systems for Homeland Security use.

14. SUBJECT TERMS CCTV, Monitoring Public Domains, Surveillance Cameras			**15. NUMBER OF PAGES** 93
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

USING SURVEILLANCE CAMERA SYSTEMS TO MONITOR PUBLIC DOMAINS: CAN ABUSE BE PREVENTED?

Thomas J. Nestel III, Staff Inspector, Philadelphia (PA) Police Department
B.S., Chestnut Hill College, 2001
M.S., St. Joseph's University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2006

Author: Thomas J. Nestel

Approved by: David Brannon
Thesis Advisor

Jerry Ratcliffe
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

After mainland United States suffered a violent attack upon its citizenry, Homeland Security professionals recognized the need to protect a growing number of critical infrastructure locations. Millions of dollars earmarked for emergency management programs were funneled into technologies that enabled public safety to "do more with less." Closed circuit television surveillance systems rocketed to the forefront as the must-have technology. Citizens of the United States became subject to video surveillance during their normal daily routines.

This thesis examines the management of CCTV systems used by municipal police departments and analyzes the policies created to control the technology and prevent abuse. Using U.S. Census Bureau data, the police departments responsible for protecting the 50 largest cities were contacted and surveyed. The initial step determined what jurisdictions utilized surveillance cameras to monitor public domains. The follow-up steps gathered information about the systems being used; the management decisions regarding where to place the cameras; the training for its operators; supervision standards; the written policies regulating the department's program; analyzing those directives; and finally, presenting step-by-step recommendations for implementing CCTV surveillance systems for Homeland Security use.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Technology enables government and public safety administrators to accomplish the number one goal of every manager—to do more with less. Random patrols of geographic areas using human assets remain limited while the implementation of CCTV technology exponentially increases the potential patrol coverage. The ability to monitor large geographic areas with minimal human resources appeals to those responsible for protecting society from criminal and terrorist behavior. The danger of watching (without detection) public areas and the curtilage of private property lies in the awesome temptation for individuals employed by private and government entities to improperly utilize the tool of surveillance camera systems.

In the quest to secure the homeland, technology automatically becomes a partner for the average beat cop. With more than 1 million CCTV surveillance cameras presently in use throughout the United States, standardized controls are necessary.[1] The potential infringement upon persons lawfully protesting, the release of images, and the ability to satisfy voyeuristic desires are real threats to the integrity of CCTV systems and organizations that use those systems.

The success of CCTV implementation to monitor public domains in American cities hinges completely on public and political acceptance. As such, the policy options analysis exists as the appropriate methodology to assess the most effective template for use by Homeland Security professionals. An historical review has been conducted by examining the policies, procedures and technologies used throughout the world. The comprehensive review will assist in determining the best methods available to accomplish the goal of protecting civil liberties and preventing abuse with CCTV surveillance systems. It is imperative that homeland security professionals act responsibly when engaging in processes that tread very close to the line protecting civil liberties.

[1] John D. Woodward, "Privacy vs. Security: Electronic Surveillance in the Nation's Capital," *RAND Corporation* (CT-194 2002): 1, http://www.rand.org/pubs/testimonies/ct194/index.html [Accessed August 2005].

The future use of technology in homeland security efforts to protect the nation relies on two elements: 1) successfully defending against legal challenges, and 2) maintaining public support. Without suitable preventive procedures and organizational acceptance of those measures, agencies utilizing CCTV surveillance cameras are likely to fail in preserving the elements that will allow development and implementation for the task of homeland security.

The limitless possibilities presented by introducing CCTV technology to the urban domain will be drastically influenced by public acceptance. Gaining community support leads to political sponsorship. If the citizens of a jurisdiction are willing to expand the social contract and permit law enforcement to utilize this tool, then the elected officials of the region will be less likely to challenge the new initiative. It is imperative that homeland security executives assure the public that sufficient controls are in place to prevent the improper use of the camera systems and recorded images. A best practices template will enable administrators to prevent civil rights violations, protect the privacy of the general public and garner the support of both allies and critics.

Until the people of the community can be put at ease regarding the police use of surveillance camera systems, the capabilities of this technology will be inhibited by controversy. The support of the American public and the unspoken agreement to provide government with the authority to deal with the dormant possibility of infringement upon basic freedoms must remain intact. The goal of this thesis lies in the desire to successfully control a potentially invasive technology. Strengthening the cooperative relationship between public safety professionals and the public hinges on how much the people trust the ability of law enforcement et al to control their own operations.

Research and formal/informal contacts identified a multitude of organizations as having CCTV surveillance cameras in their arsenal of weapons directed at fighting the global war on terrorism. Additionally, several agencies (primarily schools) were discovered that routinely use this technology in safety and surveillance applications that do not apply to homeland security. A total of twenty- six organizations using CCTV surveillance technology were contacted and a person knowledgeable in the operation of the system was interviewed A series of questions were asked in order to identify how

long the system has been in place, how the choice of camera location was made, whether the public was involved in the decision-making process, what training operators must complete, whether supervisors monitor camera operations, and whether a policy was created and disseminated.

The debate continues regarding whether CCTV surveillance systems are capable of assisting public safety professionals in reducing crime and preventing terrorism. Ongoing research may assist homeland security entities in determining if this technology serves as a useful tool in protecting society. This thesis will not participate in that value judgment argument. Regardless of what the future holds for CCTV surveillance systems, the sheer volume of cameras presently in use merits oversight attention.

Business Week conducted a survey shortly after the 9/11/01 attack in order to determine whether public support exists for intensive introduction of CCTV surveillance systems in public areas. Overwhelmingly, U.S. citizens supported any effort to create a net of surveillance, especially if it involved facial recognition technology in their cities.[2] Combine the eagerness of public safety professionals to install surveillance systems with the willingness of the public to allow that to happen, and potential abuse lurks at the turn of every camera.

Measures must be implemented to protect Homeland Security strategists from losing a potentially vital technology. This thesis will present the problems that exist in controlling video surveillance systems and the solutions presently in use throughout the world. A thorough evaluation will be launched in order to develop recommended courses of action to be taken by public safety executives contemplating the use of video surveillance in their jurisdictions.

[2] Marcus Nieto, Kimberly Johnston-Dodds, and Charlene Wear Simmons, "Public and Private Applications of Video Surveillance and Biometric Technologies," *California Research Bureau* (CRB 02-006 2002): 7, http://www.library.ca.gov/CRB/02/06/02-006.pdf [Accessed August 2005].

THIS PAGE INTENTIONALLY LEFT BLANK

II. INCREASING CCTV SURVEILLANCE

New York Senator Hillary Clinton urged New York City transit authorities to increase the number of CCTV surveillance systems monitoring the subways even though there are already more than 5,000 cameras in operation.[3] By 2006, Chicago Mayor Richard M. Daley hopes to make his video surveillance system one of the largest in the world.[4] The Pentagon spearheaded a secret plan to develop video surveillance enabling the military to track, identify and analyze the movement of every vehicle in a city occupied by U.S. troops.[5] The Department of Homeland Security earmarked millions of dollars for the introduction of surveillance systems in major cities throughout the country. In 1998, New York City's Chinatown had 13 CCTV cameras observing the public domain. In 2004, a mere six years later, the same geographic area now has more than 600 cameras.[6]

Video surveillance has blanketed the American public as a counter-terrorism tool and has become the premier weapon in public safety's arsenal. Its investigative value may be unequaled for the post-incident review. Its deterrence value may prove to be overbearing for the less motivated criminal/terrorist. As the United States quickly approaches the multi-million camera realm that has been established by the United Kingdom, precautionary measures must be introduced to prevent, deter, and address misuse of video technology by government entities. America's foundation lies on a strong belief in protecting personal privacy. Without operating policies, technological limitations, national standardization, and legal guidelines, the actions of the nefarious few will drastically impact upon those tasked with protecting the American public. These abuses are already occurring and could provide the tipping point for the wave suggesting prohibition of video surveillance in the public domain.

---

[3] Associated Press, "Step Up Surveillance, USA," *Wired News*, July 24, 2005, http://www.wired.com/news/privacy/0.1848.68296.00.html [Accessed December 10, 2005].

[4] Stephen Kinzer, "Chicago Moving to 'Smart' Surveillance Cameras," *New York Times*, sec. A, September 21, 2004, late edition.

[5] Tim Reid, "US surveillance will track every car," *Times* (London), July 3, 2003, http://www.globalsecurity.org/org/news/2003/030703-car-surveillance01.htm [Accessed August 2005].

[6] New York Civil Liberties Union, "Surveillance Camera Project," http://www.nyclu.org/surveillance_camera_main.html [Accessed December 10, 2005].

A. ABUSE AND MISUSE OF THE TECHNOLOGY

Casinos in Atlantic City (NJ) utilize state-of-the-art video surveillance equipment to assist in the detection and prosecution of thieves and cheaters. A special arm of the New Jersey Attorney General's Office, the Division of Gaming Enforcement, regulates the operation of the casinos. Due to a complaint lodged with the DGE, state officials launched an audit. After reviewing tapes of cameras monitoring the gaming area of the Caesars Atlantic City Hotel Casino, they found that more than an hour of images taped by two employees was found to be focused inappropriately on women.[7]

Several years later, the same casino submitted to a review of its surveillance tapes by the Division of Gaming Enforcement. Even though two employees had been fired in the earlier investigation and an $80,000 fine was paid to settle the complaint lodged by the victims, similar violations were discovered. Four more employees had used the legally-required hidden cameras to zoom onto specific body parts of females in the gaming area.[8]

In Tuscaloosa (AL), a surveillance camera trained on an intersection and relaying video images to a local cable TV channel changed from stationary viewing to following young women walking down the street. As the camera focused on breasts and buttocks it was transmitted live on Comcast Cable's Channel 45. Although the camera was installed by the city's department of transportation, several law enforcement agencies possessed the authority to override the stationary command of the camera. The transportation director for Tuscaloosa's Department of Transportation blamed the Alabama State Police for inappropriately directing the camera.[9] As a result of this incident, the city disabled the override function for the State Police.[10]

---

[7] John Curran, "Atlantic City casino fined for hidden cameras' wandering eyes," *Associated Press New York*, December 15, 2004, http://www.ap.org [Accessed December 2005].

[8] Associated Press, "Four surveillance camera operators at N.J. casino accused of ogling female patrons," *Associated Press New York*, April 27, 2005, http://www.ap.org [Accessed August 2005].

[9] Jon Gargis, "Strip traffic camera zooms in on bar-goers," *University of Alabama Crimson White*, September 12, 2003, http://www.cw.ua.edu/vnews/display.v/art/2003/09/12/3f629e6e6a1fd?im_archive=1 [Accessed June 2005].

[10] Associated Press, "Three Arrested After Traffic Camera Aimed as (sic) Passersby," *WAFF 48 News*, September 16, 2003, http://www.waff.com/Global/story.asp?S=1445080 [Accessed September 2005].

While on duty at his security surveillance position, an Arizona casino employee utilized his agency's technology to take breast photos of unsuspecting females. The employee received a warning for this transgression. Even after being warned, the employee engaged in the same behavior on another day. He and his supervisor were subsequently terminated from their positions with the tribal casino.[11]

A University of Nevada (Reno) professor sued his employer after university police allegedly used surveillance cameras to monitor him. Dr. Hussein S. Hussein had obtained millions of dollars in grant funding for animal nutrition research. After Dr. Hussein filed a complaint with the Department of Agriculture regarding the care of animals in the trust of the university, Hussein alleged university police notified the FBI that he was a homeland security threat.[12] Although University Police Chief Adam Garcia initially denied having control of the "Homeland Security" video system, he later admitted to issuing an order authorizing the surveillance cameras to observe the professor's office door and the hallway leading to it.[13]

A 22-year old man shot himself in the head after his relationship with a 16-year old girl failed. The incident was captured by a New York City Police Department surveillance camera. Although the image enabled police to immediately understand the circumstances of the death which occurred in the lobby of a housing project, the video found its way onto a pornographic web site. Responsibility for the video leak has been directed at the police unit assigned to monitor the surveillance cameras.[14]

New York City Councilman Hiram Montserrate, a former police officer, related in an interview that he had served with the NYPD Video Interactive Patrol Enhancement Response (VIPER) Unit.[15] Montserrate reported that he witnessed peers using video

---

[11] John Stearns, "2 at casino fired for breast photos, dealers, customers pictured," *Arizona Republic*, sec. B1, June 5, 2004, http://www.azcentral.com/news/ [Accessed August 2005].

[12] Scott Sonner, "Nevada researcher alleges university police falsely reported homeland security concerns," *Associated Press New York*, April 23, 2005, http://www.ap.org [Accessed July 2005].

[13] Frank X. Mullen, "UNR's camera network raises fear," *Reno Gazette–Journal*, sec. 1A, March 13, 2005, http://news.rgj.com [Accessed July 2005].

[14] Ikimulisa Livingston and Philip Messing, "New York Police Seek Leak of Video," *Officer.com* (April 1, 2004), http://www.officer.com/article/article.jsp?id=11339&siteSection=1 [Accessed June 2005].

[15] Sarah Wallace, "NYPD Housing Surveillance Staffed by Cops Under Investigation," *Officer.com* (April 23, 2004), http://www.officer.com/article/article.jsp?id=12078&siteSection=1 [Accessed August 2005].

technology to look into property windows or at women not suspected of any criminal activity. Montserrate stated that there were no administrative controls to prevent access to tapes; no training for camera operators; and a lack of supervisory oversight. When Montserrate reported his observations, he was transferred from the VIPER assignment.

A San Francisco (CA) police officer used the department's ultra-modern surveillance camera system at the International Airport to view the breasts and buttocks of women travelers. The officer spent three hours in the control center engaging in this behavior although he was assigned to patrol roads leading into the airport and parking areas. The officer received a 9-month suspension for his inappropriate behavior.[16]

A Tennessee school district became the target of a federal lawsuit when surveillance cameras were discovered in a school locker room. When confronted with the information regarding the placement of the school-sanctioned cameras, administrators stated that the images recorded were "…nothing more than images of a few bras and panties."[17]

The use of CCTV surveillance systems for personal gain or pleasure fans the flames of concern regarding the dangerously invasive potential of the technology. Every incident of abuse serves as a building block for limiting the government's ability to add public domain surveillance to its terrorism prevention methods. Preventing abuse can drastically improve the public's willingness to empower the government in its efforts to protect society.

B. THE FUTURE AND THE TECHNOLOGY

During the 2001 Super Bowl in Tampa Bay, Florida, 19 petty criminals were identified by CCTV surveillance cameras equipped with biometric software[18] Since regulations do not exist on the use of this technology, a casino could identify persons who

---

[16] Bay City News, "SF cop who reportedly ogled women is suspended for 9 months," *SFGate.com*, April 21, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/ baycitynews/ archive/2005/04/21/cop21.DTL [Accessed June 2005].

[17] Amanda Wardle, "Company denies charges," *Nashville City Paper*, August 1, 2003, www.nashvillecitypaper.com/index.cfm?section_id=9&screen=news&news_id=25248 [Accessed December 10, 2005].

[18] Patrick Marshall, "Privacy Under Attack," *Congressional Quarterly* 11, no. 23 (June 15, 2001): 512.

had previously shown a connection between alcohol intake and heavier betting. By doing this, the casino could target the potential high roller for free adult beverages. Imagine shopping in a supermarket and hearing over the public address system commercials and sale announcements for products. Since regulations do not exist on the use of this technology, a supermarket could tailor its sale announcements and product commercials based on the shoppers identified in the store and their past purchase patterns. Consider technology in the hands of a jealous spouse. Since regulations do not exist on the use or release of images, requests could be made for travel routes, times of visits, and pictures of vehicle occupants based purely on a specific vehicle license number.

C. CRIMINOLOGICAL THEORY AND ITS APPLICATION TO VIDEO SURVEILLANCE

According to the routine activity theory of criminology, criminal incidents occur when three spheres converge. The three factors that are necessary to enable prohibited behavior are: 1) the motivated offender, 2) a suitable target, and 3) absence of a capable guardian.[19] In the Homeland Security arena, the offender exists as a result of religious or political ideology. Preventing the motivated offender becomes a huge undertaking that involves the tireless efforts of diplomats, mediators and religious leaders. In crime control, minimizing the potential for motivated offenders requires social service intervention. Drug and alcohol rehabilitation, anger management, behavioral modification, employment services, etc. become issues that the broad-thinking criminal justice professional must engage in order to reduce the number of motivated offenders.

Unlike the intangible ideologies and the social service concerns, reducing suitable targets can be an observed accomplishment. Hardening potential targets usually requires changing the physical structure or improving the visible security measures surrounding the structure. The number of critical infrastructure locations continues to multiply and the cost of hardening the targets is astronomical. Since the process of target-hardening is a never-ending process, the likelihood of reasonably reducing the number of suitable targets remains slim.

[19] Francis Cullen and Robert Agnew, *Criminological Theory* (Los Angeles: Roxbury, 2003), 269.

Capable guardianship endures as the sphere that public safety professionals can influence most effectively and efficiently. This particular realm of the routine activity theory purports that communities possessing active oversight tend to be victimized by less criminal activity. Capable guardianship within the neighborhoods of our cities has been left to the supervision provided by parents, concerned adults and law enforcement.[20] Technological advances have dramatically changed the capable guardian sphere for homeland security threats. CCTV surveillance of public areas can supplement or possibly replace human supervision in the terrorist prevention model.

Most criminologists assert that the pool of motivated offenders will always exist and that attention needs to be directed towards minimizing suitable targets for crime and increasing the level of capable guardianship.[21] The cost and success of hardening the variety of potential terrorist targets can make the mission of neutralizing this sphere unreasonable. This author presents the belief that the most effective and efficient manner of exercising the routine activities theory of criminology to homeland security is by using CCTV surveillance as capable guardianship.

D. CREATING PANOPTICON CITIES

An 18th century prison style known as the Panopticon enabled guards to monitor prisoners in a manner that prohibited the inmates from knowing when and from where they were being watched.[22] CCTV surveillance systems operate in much the same manner. The persons tasked with using cameras to observe behavior in the public domain can do so without detection. The end result of the Panopticon prison style and urban CCTV surveillance systems is the deterrent value.[23] Rather than committing actual physical resources to patrol an area of concern, communities can install surveillance cameras to foster the perception that someone is always watching. In order to be an effective deterrence tool, publicity and intense communication through informal

---

[20] Curt Bartol and Anne M. Bartol, *Delinquency and Justice* (Upper Saddle River, NJ: Prentice Hall, 1998), 231.

[21] Cullen and Agnew, *Criminological Theory*, 269.

[22] Katherine Williams and Craig Johnstone, "The Politics of the Selective Gaze: Closed Circuit Television and the Policing of Public Space," *Crime, Law & Social Change* (September 2000): 191.

[23] Hille Koskela, "'Cam Era'- the contemporary urban Panopticon," *Surveillance & Society* (2003): 297, http://www.surveillance-and-society.org/articles1(3)/camera.pdf [Accessed May 2005].

neighborhood networks must occur. The subjects of the unobserved surveillance must believe that inappropriate behavior will lead to a reaction from law enforcement.

Panopticon communities are slowly being developed by overlapping camera coverage of geographic zones. In Philadelphia (PA), an endeavor has begun by the police department to plot the location of every privately-owned surveillance camera on an interactive map.[24] Once the project of documenting every camera is completed, a spatial analysis will be conducted. That analysis will note the range of view for each camera and will subsequently indicate the zone of coverage available for review by law enforcement. By documenting the range and location of every camera privately and publicly operated in Philadelphia, future decisions regarding camera installation by city government can avoid duplication of coverage. Additionally, detectives will have a list of potential "witnesses" to cull during investigations of criminal and terrorist acts.

A somewhat different twist on the same idea is occurring in New York (NY). The American Civil Liberties Union has recruited college interns to conduct visual surveys of specific geographic areas as part of the "Surveillance Camera Project."[25] As noted on the New York Civil Liberties Union website, the project goal lies in the hope of stimulating citizen awareness and debate regarding the proliferation of unregulated surveillance cameras monitoring the public domain.

The New York Surveillance Camera Players have conducted their own survey of cameras in the public domain. The group formed to "protest against the use of surveillance cameras in public places because the cameras violate our constitutionally protected right to privacy."[26] Their website lists 14 different geographic areas in New York City and maps the surveillance cameras monitoring those areas.[27] This group has also conducted similar surveillance camera surveys in other major cities throughout the United States.

---

[24] Stacey Irving (Senior Director of Crime Prevention Services—Center City District—Philadelphia, PA), interview by author, Philadelphia, PA, August 10, 2005.

[25] New York Civil Liberties Union, "Surveillance Camera Project," http://www.nyclu.org/surveillance_camera_getinvolved.html [Accessed December 10, 2005].

[26] Surveillance Camera Players, "Who we are & why we're here," http://www.notbored.org/generic.jpg [Accessed December 10, 2005].

[27] Surveillance Camera Players, "Maps of Publicly Installed Surveillance Cameras in New York City," http://www.notbored.org/scp-maps.html [Accessed December 10, 2005].

Even schools have engaged in the effort to establish a protective video net over their properties and their students. Many districts have a variety of systems in place to monitor behavior of students and teachers, but the Reynoldsburg (OH) school district has offered local law enforcement live video feed of school hallways and student areas. This policy allows the police to monitor in real time what occurs in the educational facilities of that jurisdiction.

E. THE EVOLUTION OF CCTV SURVEILLANCE

These technology advancements did not occur overnight. In the United States, the origin of CCTV surveillance systems evolved differently from their introduction on the European continent. American cameras originated as passive, unmanned devices installed in banks and stores that were open throughout the night. English cameras were an active, constantly monitored technology that viewed public areas. American cameras focused on recording violent offenses, while British equipment concentrated on capturing petty thieves and vandals.

In the late 1960s and early 1970s, government funding enabled CCTV surveillance camera pilot programs in Hoboken (NJ) and Mount Vernon (NY).[28] Both cities suffered from a rash of serious crime. Surveillance systems were thought to be a cutting edge method for assisting the police in their endeavor to reduce crime. The results of the programs failed to support the belief that CCTV surveillance systems could perform as useful crime prevention tools. Nonetheless, a series of cities introduced the technology to their cache of weapons to thwart the criminal element. A variety of issues resulted in the failure of these early pilot programs. As with most government-funded initiatives, grants enabled the purchase of the equipment, but the costs of maintaining and operating the systems became the responsibility of the agency obtaining the grant. Budgetary constraints, lack of success in reducing crime, and insufficient staffing commitments resulted in wholesale abandonment of high quality government-operated

[28] Marcus Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" *California Research Bureau* (1997): 12, http://www.library.ca.gov/CRB/97/05/crb97-005.pdf [Accessed August 2005].

CCTV surveillance systems in American cities. What remained in the United States were low grade video systems in banks and businesses that were used as proof for employee thefts and investigations of robberies.

During the mid-1970s, London introduced video surveillance to its public transportation hubs and for traffic monitoring.[29] In 1986, a town in Great Britain began the first significant attempt at monitoring public domains with CCTV surveillance systems. Government officials in King's Lynn utilized cameras to monitor a very small geographic area that suffered from a pattern of minor crimes.[30] This project became the foundation for using technology to supplement the community's capable guardianship assets. The overwhelming success of this effort to help reduce crime became the catalyst for government-subsidized systems throughout the European country. As the desire increased for CCTV surveillance systems throughout England, more than 75% of the United Kingdom's Home Office spending for crime prevention efforts was spent on CCTV initiatives.[31] England has evolved as the country with more cameras per capita than any other country in the world. In the period between 1999 and 2001, the British government distributed $250 million for CCTV installation; as of 2002, there were more than 40,000 CCTV units operating in the United Kingdom.[32] It is believed that Britain presently uses more than 4.2 million cameras at an expense of $325 million to monitor the public domain.[33]

A variety of other countries in North America, Europe and Asia utilize CCTV surveillance systems in crime control and terrorism prevention efforts. In the early 1990s, Canada initiated CCTV surveillance cameras to monitor public areas.[34] The evolution of Canada's surveillance camera use mirrored its southern neighbor. What

---

[29] Michael McCahill and Clive Norris, "CCTV in Britain," *Center for Criminology and Criminal Justice,* University of Hull-UK, March 2002), http://www.urbaneye.net [Accessed July 2005].

[30] Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" 6.

[31] Brandon C. Welsh and David P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime: Protocol for a Systematic Review," *Campbell Collaboration Crime and Justice Group* (2003): 3, http://www.campbellcollaboration.org/doc-pdf/cctv.pdf [Accessed June 2005].

[32] Ibid.

[33] Associated Press, "A Look at the New Orleans' CCTV System," http://www.securityinfowatch.com/article/article.jsp?id=3318&siteSection=427 [Accessed April 17, 2005].

[34] Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" 9.

began as an effort to reduce robberies in banks and stores morphed into the monitoring of mass transit mediums, public areas and eventually border checkpoints. Like America, Canada initially used CCTV surveillance systems in crime suppression but later focused on terrorism issues. France's focus for CCTV surveillance systems has been to combat terrorist activity. The French embarked on strategic placement of cameras to actively monitor municipal buses, trains and train stations, and airport terminals.[35] In Northern Ireland, the British military uses video surveillance to monitor the Catholic areas of Belfast.[36] In addition to the military operations, the Irish have utilized private CCTV systems since the 1980s to observe shopping areas, post offices and banks.[37] Like the French, Northern Ireland has installed cameras along their public and commercial rail lines. According to research conducted by Marcus Nieto, Spain uses video surveillance to monitor public areas in order to combat terrorism and street crime. Russia and Italy utilize the technology to view government properties and tourist areas. Nieto also reports that China and Iran use CCTV covertly to observe their citizens.

CCTV operations are spreading across the world in the private and public sectors. Systems are used to prevent crime, assist in investigating criminal offenses, reduce the need for human resources and increase homeland security protection grids. Legal and professional standards should be implemented to solidify the public's faith in the ability of government to protect civil liberties as technology evolves.

---

[35] Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" 9.

[36] Nils Zurawski, "I Know Where Your Live!-Aspects of Watching, Surveillance and Social Control in a Conflict Zone," *Surveillance & Society* (2005): 508, http://www.surveillance-and-society.org/ articles 2(4)ni.pdf [Accessed September 2005].

[37] Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" 9.

III. EARLY SOCIETY'S LEGAL STANDARDS

In ancient societies, customs and traditions provided behavior guidelines for tribes and communities. Although unwritten, the rules guided loosely knit groups of people to act in a manner that protected the property and well-being of group members. Written edicts of conduct followed with the Code of Hammurabi, the Mosaic Code, and the Twelve Tables.[38] The Code of Hammurabi was chiseled on rock columns in 2100 B.C.[39] In 1200 B.C., the Mosaic Code became the foundation for American law.[40] In 450 B.C., the Roman Empire published the Twelve Tables which every Roman citizen was required to memorize.[41]

The codes and tables possessed authority in the community because of social contracts. Philosophers Thomas Hobbes and John H. Laub defined social contracts as the willingness of a population to voluntarily sacrifice a small amount of individual rights in order to enable the government to maintain control.[42] This sociological process developed during people's migration to cities and served as the focal point for civilized living.

The success of the social contract hinges on the faith that citizens have in their government. In the realm of video surveillance for the public domain, acceptance of government-operated programs remains crucial in maintaining the social contract. If support does not exist, then the social contract between citizens and their government becomes strained. As distrust increases, then pressure surfaces to introduce controls to limit the capabilities of government. Programs such as video surveillance may become potentially volatile without faith in government entities.

---

[38] Allison Payne, "Introduction to Criminology" (lecture, University of Pennsylvania, Philadelphia, PA, September 13, 2004).

[39] Stephen Light, *Understanding Criminal Justice* (Belmont, CA: Wadsworth Publishing, 1999), 74.

[40] Ibid, 75.

[41] Ibid.

[42] Ibid, 96.

A. PUBLIC SUPPORT

Studies have been conducted around the world to determine if public support exists for government surveillance systems. Research conducted in Australia by Ditton and Short (1998) and Ditton (2000) revealed that not only did such support exist, but it was overwhelming.[43] During the early stages of CCTV, English surveys showed that a very small percentage of people were concerned about government surveillance systems being used for the infringement of civil liberties. In the mid 90s, a Glasgow poll showed a 95% acceptance rate for public surveillance systems.[44] More recent English surveys have consistently shown an acceptance rate of more than 65% for those asked if they support CCTV surveillance systems.[45] An article written in the Norwegian newspaper *Aftenposten* related that 66% of Norwegians surveyed about CCTV surveillance systems support their use.[46]

Although the citizens of the world clearly support the implementation of CCTV surveillance, a growing number of people express concern about the potential for abuse. As CCTV becomes more widely used, trepidation increases regarding the lack of control or oversight for the technology. A German survey conducted during the summer of 2003 by the Berlin Institute for Social Research found that 65% of the people interviewed felt that CCTV systems presented a potential for abuse.[47] The same survey found that people strongly desire the implementation of strict regulations for the release and storage length of video images, as well as inspection, registration and licensing of systems.

B. CCTV LAW IN THE UNITED KINGDOM

Although Great Britain led the world in the use of CCTV surveillance systems, the country reacted slowly to introduce legislation that could control the public domain

---

[43] Dean Wilson and Dr. Adam Sutton, "Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation," *A Report to the Criminology Research Council* (November 2003): 5.

[44] Phillip Edwards and Nick Tilley, "Closed Circuit Television Looking Out For You," *Home Office Police Research Group* (1995), http://www.homeoffice.gov.uk [Accessed April 2005].

[45] McCahill and Norris, "CCTV in Britain," 20.

[46] Ann Rudinow Saetnan, Johanne Yttri Dahl, and Heidi Mork Lomell, "Views from under surveillance. Public opinion in a closely watched area in Oslo," *Urbaneye Project* (January 2004), http://www.urbaneye.net [Accessed May 2005].

[47] Frank Helten and Bernd Fischer, "What Do People Think About CCTV? Findings From a Berlin Survey," *Berlin Institute for Social Research* (February 2004): 18.

observations. The Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, and the Data Protection Act 1998 had elements that specifically regulated CCTV operations.[48]

- The Human Rights Act 1998 included two sections that applied to the use of CCTV surveillance systems. The first section, Article 6, addressed the right to a fair trial. The second, Article 8, protected the right to respect for family and private life. The Act established British law that allowed surveillance video of the public domain to be used in criminal cases.[49]
- Specifically drafted to control government CCTV operations, the Regulation of Investigatory Powers Act (RIPA) 2000 provided legal guidelines for police agencies. The act required that CCTV surveillance be proportionate, legal, accountable, and necessary. This legislation required supervisory oversight and meticulous record keeping.[50]
- The Data Protection Act 1998 required that the installation and operation of CCTV systems to monitor public domains had to be done in conformance with a specific legal basis. The act also required any government or private entity to register surveillance systems with the Data Commissioner.[51] This legislation prohibits the release of images except for purposes of crime prevention and detection.[52] The act required every CCTV surveillance system to be registered with the Information Commissioner and to be operated using the principles of openness, fairness and proportionality.[53]

In July 2000, the British Data Commissioner issued a document entitled, "CCTV Codes of Practice." This government missive provided data protection rules for the gathering, storage and protection of CCTV images. In order to ensure that every CCTV camera system operated in compliance with the Code, every system had to be registered with the government by 2003.[54] This major set of guidelines requires all persons utilizing surveillance camera systems to:

- install cameras at locations based on specific crime or public safety needs

---

[48] McCahill and Norris, "CCTV in Britain," 4.

[49] Ibid, 52.

[50] Ibid.

[51] Ibid, 53.

[52] Parliamentary Office of Science and Technology, "CCTV," *Postnote*, no. 175 (April 2002): 4, http://www.parliament.uk/post/pn175.pdf [Accessed June 2005].

[53] Marianne L. Gras, "The Legal Regulation of CCTV in Europe," *Surveillance & Society* (2004): 217, http://www.surveillance-and-society.org/articles2(2)/regulation.pdf [Accessed May 2005].

[54] Ibid.

- use the system for the stated purpose and not for other labor or employee performance reasons
- be able to view only the areas related to the problem and not surrounding private property
- maintain records showing access and chain of custody for all images
- adhere to retention restrictions for images
- allow image subjects to obtain copies of any and all images
- implement safeguards to prevent improper access to images[55]

Based on a claim of invasion to privacy allegedly committed by police authorities in Great Britain, the European Commission of Human Rights ruled that images taken of a person in a public area do not constitute a privacy violation as long as the images are not made available to the general public.[56]

Similar to the American system of justice, English law often develops when magistrates interpret legislation as it applies to actual incidents. Deliberation in criminal courts provides judges with the opportunity to decide how a law was intended to regulate society. Technological advances periodically stretch the boundaries of the written law. When the English rules of evidence were established regarding images, photographs were among the items considered by the lawmakers. CCTV surveillance system pictures unveiled a new ability to capture the actions of persons over a wide range of area. In 1982, English courts (R v. Grimer and R v. Fowden and White) decided that this new technology should possess the same validity as that of an eyewitness observation.[57]

C. CCTV STANDARDS IN THE UNITED KINGDOM

In addition to legal standards established to control CCTV systems in England, informal guidelines were published for private companies considering the implementation of this technology. The guidelines have no legal standing but are published by the Home Office as a resource for private and public organizations considering the introduction of CCTV.

---

[55] McCahill and Norris, "CCTV in Britain," 54.

[56] Ralph Beddard, "Photographs and the Rights of the Individual," *Modern Law Review* 58, no. 6 (November 1995): 780.

[57] James Sheptycki, "Surveillance, Closed Circuit Television and Social Control," *Policing and Society* 9 (2000): 430.

The Home Office guidelines offer private entities the opportunity to utilize the police as consultants and advisors in the implementation of CCTV schemes. In its efforts to successfully introduce CCTV surveillance systems to the public domain, the political leadership of the United Kingdom encourages the use of the Police Service. The guidelines state that law enforcement professionals are available to evaluate the need for CCTV; establish a code of practice; train operators; develop command and control formats; encourage community support; and conduct spot checks during operational periods.[58]

D. CCTV LAW IN THE UNITED STATES

When it comes to U.S. Federal law, there is little that specifically applies to regulating CCTV surveillance systems. The primary issue attached to the CCTV debate lies in the belief that Americans have a right to privacy. The Constitution of the United States does not guarantee a right to privacy. The Fourth Amendment provides protection against unreasonable searches and seizures, but it does not limit actions that private citizens can engage in that directly affect another person's privacy. The legal restrictions apply only to actions precipitated by the government and arguably limit infringement upon privacy, but they do not provide a right to that privacy. The courts have ruled that government entities may observe public areas because no expectation of privacy exists. Technology may be used to conduct video surveillance but not to intercept communication between people. The Electronic Communications Privacy Act of 1986 requires a search warrant in order to monitor conversations in the public arena.[59]

The key piece of legislation empowering government agencies to conduct CCTV surveillance over public domains lies in the 1967 Supreme Court case, Katz v. United States.[60] In that case, the Court ruled that a reasonable expectation of privacy test should be applied in order to determine if a government search was illegal. The test required answering two questions: did the subject of the search have an expectation of privacy and would society agree upon the subject's belief that the expectation was reasonable.

---

[58] Edwards and Tilley, "Closed Circuit Television Looking Out For You."

[59] Patrick Marshall, "Privacy Under Attack," 513.

[60] Nieto, Johnston-Dodds, and Simmons, "Public and Private Applications of Video Surveillance and Biometric Technologies," 38.

Only if both questions were answered in the affirmative would there be reason to acquire a search warrant before seizing evidence. Second millennium societal beliefs do not hold that public spaces provide an individual with an expectation of privacy. Due to this existing mindset, the use of video technology to monitor public areas would not be in violation of the Fourth Amendment to the United States Constitution.

In 2001, the Supreme Court pondered the government's use of technology to gain information regarding criminal wrongdoing allegedly occurring inside private property. In Kyllo v. United States, the police used a device capable of conducting thermal imaging detection in order to ascertain if a homeowner was using powerful lights to facilitate the growth of marijuana.[61] The court ruled that a warrant was necessary if the government utilized a device "not in general public use" to make observations of a private property that could not have been made without entering the property.[62] An argument could be presented that the results of this case limit the use of CCTV surveillance systems. The flaw in such a claim is that as time progresses, CCTV surveillance systems have become a commonly used technology thus negating the "not in general public use" clause of the Supreme Court's decision.

A variety of unintentional personal data releases prompted Congress and several state legislatures to enact protective edicts forcing credit card companies and retail establishments to shield consumer information. The laws have not bridged the gap that divides personal information with video images that reflect a person's appearance. Although significant concern exists to protect the privacy issues related to a person's purchase patterns and medical records, little concern has surfaced regarding CCTV surveillance systems.

The research for this thesis included contacting the police departments of the nation's 50 largest cities. The municipalities that utilize CCTV surveillance systems to monitor the public domain have no legal guidelines regulating the system's control, operation, training, or release of images. This research found neither legal challenges nor indications of judicial support for privacy arguments applying to public spaces.

[61] Nieto, Johnston-Dodds, and Simmons, "Public and Private Applications of Video Surveillance and Biometric Technologies," 39.

[62] Kyllo v. U.S., 121 S. Ct. 2038 (2001).

Nevertheless, as the number of covert camera schemes increase, laws to limit their use must be developed. One such example of this phenomena occurred in Long Island, New York. Stephanie Fuller was victimized by a voyeuristic landlord who installed a video camera in her bedroom.[63] Since there were no laws prohibiting invasion of privacy behavior, the victim initiated a change in legislation. The change made covert video surveillance conducted for amusement, entertainment or voyeuristic purposes a class D felony punishable by 2 to 7 years in prison.[64]

E. CCTV STANDARDS IN THE UNITED STATES

The United States has a variety of professional organizations that provide operational and administrative guidance for its members. Four major law enforcement organizations developed an accrediting agency to assist departments in creating and maintaining professional standards. The Commission on Accreditation for Law Enforcement Agencies (CALEA) provides a rigorous certification process for the nation's police departments. As of December 2005, the only CALEA standards regulating CCTV in organizations that submit to the certification process include the following:

- **72.8.2** If audio and/or visual surveillance equipment is used, a written directive specifies that the equipment will be controlled to reduce the possibility of invading a detainee's privacy.
- **41.3.8** If agency-owned, in-car audio or video recording systems are used, a written directive establishes policy and procedures for the following:
  - a) situations for use
  - b) tape security and access
  - c) tape storage and retention
- **43.1.4** A written directive establishes a system for the authorization, distribution, and use of surveillance and undercover equipment.
- **83.2.2** A written directive governs procedures used for photography and video taping pursuant to the collection and preservation of evidence and specifies the information to be recorded at the time this tape is taken.[65]

---

[63] "Stephanie's Law Creates Criminal Penalties for Covert Use of Viewing Devices on Unsuspecting Victims," *New York State Governor's Press Releases*, June 23, 2003, http://www.ny.gov/governor/press/03/june23_1_03.htm [Accessed June 2005].

[64] Ibid.

[65] "2005 CALEA Standards Manual," *Commission on Accreditation for Law Enforcement Agencies*.

Since legal guidelines do not yet restrict the use of CCTV surveillance systems, the Justice Department issued policy guidelines for video surveillance by government agencies. The standard presents the opinion that the existing Federal Wiretap Act (Title III) does not control the use of CCTV systems. It also notes that requests for search warrants permitting the use of video surveillance have been held to a higher standard in six of the circuit courts.[66]

Foreseeing the increased use of technology in the investigation and prosecution of criminal cases, the American Bar Association developed a set of standards entitled "Technologically-Assisted Physical Surveillance." Standard 2-9.1 states that the need for regulation arises because technology can "diminish privacy, freedom of speech, association and travel, and the openness of society."[67] The committee responsible for the drafting of the document did not recommend prohibiting CCTV video surveillance of public domains. Instead, the guidance directed law enforcement officials to coordinate with the citizens of the area where the proposed video coverage would extend. The collaboration would include advising the citizens of the intended location of the camera and its capabilities. Additionally, public meetings should be held so that the value of the continued surveillance could be evaluated or improved upon. The standard strongly recommended the development of administrative controls and protocols for the storage and release of images.

F. CCTV LAW IN OTHER EUROPEAN COUNTRIES

Member countries of the European Union are required to blend legal standards established by the EU into their own country's legislative restrictions. The European Data Protection Directive 95/46 uses language that could be applied to the CCTV issues.[68] In July 1982, Danish lawmakers restricted private video surveillance of

---

[66] Nieto, Johnston-Dodds, and Simmons, "Public and Private Applications of Video Surveillance and Biometric Technologies," 50.

[67] *American Bar Association Standard 2-9.1(b).* "Electronic Surveillance: Technologically-Assisted Physical Surveillance," Adopted 1998.

[68] Carsten Wiecek and Ann Rudinow Saetnan, "Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark," *Urbaneye Project* (March 2002), http://www.urbaneye.net [Accessed July 2005].

publicareas.[69] Although this legislation does not address government use of CCTV technologies, section 264 of the Penal Code provides two guidelines for public officials:

- the surveillance is necessary as part of a continuing investigation
- the offense is punishable by 18 months or more of imprisonment.[70]

Norway does not participate in the European Union but has used that compact's directives in the formation of law. The EU Data Protection Directive appears to be the genesis for Norway's Personal Data Act which was released in January 2001.[71] Although the Act does not specifically mention CCTV surveillance systems, it has been interpreted to apply to this technology. As such, the registration requirement for operation of CCTV systems must be completed by persons wishing to utilize this type of surveillance.

German law strictly regulates the use of video surveillance for the public domain.[72] A 1983 decision determined that in order to have a democratic society, persons must know why they are the subject of surveillance and by whom they are being watched.[73] German police are permitted to conduct surveillances related to criminal activity or of areas that are high threat but are not allowed to permanently affix surveillance cameras to observe public areas. The topic of CCTV surveillance generated a decade of volatile political debate in Germany which was resolved in January 2003 with the Police and Public Order Act. The act permitted the police to monitor areas of high threat and to permanently store images from those identified locations.[74] An interesting twist in German law limits private CCTV surveillance system use. A store owner can utilize covert surveillance cameras to enable employees to prevent a crime from

---

[69] Carsten Wiecek and Ann Rudinow Saetnan, "Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark," *Urbaneye Project* (March 2002), http://www.urbaneye.net [Accessed July 2005]

[70] Ibid.

[71] Ibid.

[72] Helten and Fischer, "What do people think about CCTV? Findings from a Berlin survey," 4.

[73] Eric Topfer, Leon Hampel and Heather Cameron, "Watching the Bear," *Urbaneye Project* (December 2003), http://www.urbaneye.net [Accessed July 2005].

[74] Topfer, Hampel and Cameron, "Watching the Bear."

occurring. Systems that merely record evidence of a crime that was permitted to occur are deemed to be a form of entrapment and therefore illegal.[75]

The Austrian Constitution does not provide an individual right to privacy.[76] Austria has an extensive traffic safety surveillance system that monitors roadways and tunnels. Several laws exist that regulate the use of audio and video surveillance equipment but none of it restricts the authority of the police to conduct monitoring of public areas.

Swiss law does not have any provisions that regulate the operation, management or control of government owned CCTV surveillance systems.[77] Legal cause must exist in order for Swiss authorities to utilize CCTV technology. In order for video surveillance to be authorized along the country's border, legislation had to be crafted to permit such activity. An exception to the need for legislative action for video surveillance would be "in the case of danger or of an overt risk."[78]

In France, CCTV surveillance systems must be approved by a panel consisting of judges and elected officials from the geographic area. The application process must be completed for every private institution wishing to introduce CCTV surveillance to either the work environment or the public domain. Police agencies are exempt from the legal requirement of surveillance system registration.

Canada addressed the admissibility of CCTV surveillance camera images following the hockey riots of 1994 in Toronto. According to *Anatomy of Crime*, government cameras recorded several hundred unknown citizens engaging in criminal activity.[79] The images were posted on web sites and publicized through the media. The Canadian courts ruled that CCTV images should be valued more than a human eyewitness. In the months following the destruction in Toronto, 161 people were

---

[75] Gras, "The Regulation of CCTV in Europe," 220.

[76] Steven Ney and Kurt Pichler, "Video Surveillance in Austria," *Urbaneye Project* (April 2002), http://www.urbaneye.net [Accessed July 2005].

[77] Jean Ruegg, Valerie November and Francisco Klauser, "CCTV, Risk Management and Regulation Mechanisms in Publicly-Used Places: A Discussion Based on Swiss Examples," *Surveillance & Society* (2004): 420, http://www.surveillance-and-society.org/cctv.htm [Accessed May 2005].

[78] Ibid.

[79] Court TV, December 28, 2005.

arrested. Because of the video evidence, all but one pled guilty. The remaining individual was subsequently convicted for his involvement in the riots.

A variety of laws and standards exist throughout the world to regulate CCTV surveillance systems. It is evident that the longer a society submits to video technology monitoring the public domain, the more controls and regulations are enacted. Oliver Wendell Holmes said, "The law embodies the story of a nation's development through many centuries."[80] U.S. Homeland Security professionals should heed the lessons learned by its European allies. Laws and standards should be created by public safety administrators to minimize the possibility of CCTV surveillance system abuse.

[80] Ronald J. Allen and others, *Criminal Procedure*, (New York: Aspen Publishers, 2005), 277.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SURVEYS OF ORGANIZATIONS USING CCTV

This author sought guidelines and policies already in place regulating CCTV surveillance systems in the United States. The most common public and quasi-public organizations using video surveillance are police departments and school districts. In the private realm, the business best known for its use of actively monitored CCTV surveillance is the casino industry.

During the literature review for this thesis, thirty-seven (37) police departments, school districts and casinos were identified as having CCTV surveillance systems in their arsenal of tools to thwart crime and terrorism. In addition to the agencies identified during the thesis research, the author contacted the police departments for the fifty (50) most populated municipalities in the United States to ascertain which organizations utilize public domain surveillance systems. As of February 15, 2006, the responses from the police departments of the fifty (50) most populated municipalities are as follows:

- Seventeen (17) are utilizing surveillance systems in the public domain
- Nineteen (19) are not utilizing surveillance systems in the public domain
- Fourteen (14) have not responded to requests for information

A total of twenty-three (23) organizations expressed a willingness to participate in the survey process used for this thesis. Three departments have surveillance systems but did not participate in the survey. New Orleans (LA) declined due to their ongoing priority of recovering from Hurricane Katrina. Sacramento (CA) and Long Beach (CA) are both in the development stage of introducing surveillance systems to their jurisdictions.

The contact person for each of the noted agencies agreed to submit to a survey. The questionnaire was crafted to understand the size of the target agency, the length of time that CCTV operations have been in operation, and to identify methods to prevent abuse of the technology. During the interview process, the contact persons answered the following questions:

- How long the organization has used CCTV surveillance cameras
- How many cameras made up the organization's surveillance system

- How the agency decided where to install surveillance cameras
- Whether the cameras are actively or passively monitored
- Whether the cameras are operating 24 hours/7 days a week
- Whether the organization has a policy for CCTV operations
- Whether the community had input in the implementation process
- What the training entailed for CCTV operators
- Whether there is constant supervision of CCTV operations
- How the decision is made regarding the release of images
- How long images are saved
- Whether the system would be used to prevent a crime or serve as evidence after the crime
- Whether any state or local laws exists regulating CCTV operations
- Whether private CCTV operations must register with a government agency
- How the agency prevents abuse of the CCTV operation
- Whether the agency has received any complaints regarding its CCTV operation
- Whether images have been successfully used for criminal prosecutions

A. ALEXANDRIA (VA) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for eighteen years and the operation includes more than sixty cameras. The cameras were installed at locations determined by a security consultant. The system is actively monitored and operates on a 24/7 basis. A written policy for operations does exist however it was unavailable for review. The community was not involved in the initial or subsequent implementation process. The only training available to the CCTV operators is on-the-job training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the Division Chief for review. The images are saved until storage space is no longer available. At this time, it is believed that storage space will never be an issue. The operators have not been trained on what to do if an operator observes a suspicious person checking car doors. The contact person in Alexandria did not know if any state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems must obtain certification through the Commonwealth of

Virginia. Enforcement of the written policy prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have not yet been used in any prosecutions for criminal behavior.

B. ANCHORAGE (AK) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for more than ten years and the operation includes six cameras. The cameras were installed at locations determined by the department. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. The only training available to the CCTV operators is on-the-job training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the Chief for review. The images are saved until storage space is no longer available. At this time, it is believed that storage space will never be an issue. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlled access to the system prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have not yet been used in any prosecutions for criminal behavior.

C. ATLANTA (GA) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for one year and the operation includes more than thirty cameras. The cameras were installed at locations chosen by the department and by the funding sources. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. The only training available to the CCTV operators is on-the-job training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the Public Affairs Division for review. The images are saved for 90 days. If an operator observes a suspicious person checking car doors, the operator waits until the

crime is committed before taking action. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center and constant video monitoring of the operators prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used to successfully prosecute more than twelve criminal cases.

D. BALTIMORE (MD) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for four years and the operation includes more than two hundred cameras. The cameras were installed at locations chosen by the department. The system is actively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was involved in the initial and subsequent implementation process. The only training available to the CCTV operators is on-the-job training. Constant supervision exists for West Side cameras but not for other areas of the city. Any requests for images are forwarded to the State Attorney's Office. The images are saved for 28 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Security companies are required to be licensed through the state. Close supervision prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used to successfully prosecute several criminal cases.

E. CENTENNIAL SCHOOL DISTRICT (PORTLAND, OR)

The school district has been utilizing CCTV surveillance systems for more than ten years and the operation includes more than eighty cameras. The cameras were installed at locations based on input from school staff. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. CCTV operators receive special training. Constant supervision does not exist for CCTV operations. Any request for images will be granted upon written request. The images are

saved for 14 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. The contact person did not know if state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. No measures have been taken to prevent abuse. The school district has not received any complaints from the public regarding the use of its cameras. Recorded images have been used to successfully prosecute criminal behavior.

F. CHARLOTTE-MECKLENBERG (NC) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for fifteen years and the operation includes more than one hundred cameras. The cameras were installed at locations chosen by the department in coordination with downtown building owners. The system is actively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. CCTV operators receive special training. Constant supervision does exist for CCTV operations. Requests for images must be made in writing and are evaluated by the Chief. The images are saved for 3-5 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. The small number of persons authorized to access the system prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

G. CHICAGO (IL) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for two and a half years and the operation includes more than one hundred cameras. The cameras were installed at locations chosen by the department. The system is actively monitored and operates on a 24/7 basis. A written policy entitled Operation Disruption Video

Surveillance Pilot Program and dated August 5, 2003 does exist for CCTV operations and includes the following elements:

- A Deputy Chief is designated as being the pilot program director
- Field supervisors and personnel assigned to monitor video surveillance must receive special training
- Limits operation of cameras to trained personnel only
- Cameras are to be put on automatic mode when not being directly monitored
- Training consists of 1st Amendment, 4th Amendment, consent search issues and proper operation of the surveillance equipment
- Requests for retrieval of images will be initiated by a supervisor and submitted on a Retrieval Request Form
- Copied images will be entered into the Evidence and Recovered Property Section

The community was not involved in the initial or subsequent implementation process. Special training advises employees of the technical capabilities of the software and hardware. Refresher courses are held reminding personnel of the 1st Amendment and 4th Amendment issues. Constant supervision does not exist for CCTV operations. Any requests for images are submitted by a supervisor through the chain of command by completing a Retrieval Request Form. The images are saved for 72 hours. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. The contact person in Chicago did not know if private agencies wishing to utilize CCTV systems are required to register with any government agency in the jurisdiction. Training, close supervision, and controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used to successfully prosecute several criminal cases.

H. DALLAS (TX) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for two and a half years and the operation includes more than eighty-five cameras. The cameras were installed at locations chosen by the department. The system is passively monitored and

operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. The vendor provides training to the CCTV operators and on-the-job training occurs with a technician. Constant supervision does exist for CCTV operations. Any requests for images are forwarded to the Chief who abides with the provisions of the Sunshine Law. The images are saved for 60-90 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have not yet been used in any prosecutions for criminal behavior.

I. FRESNO (CA) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for less than one year and the operation includes more than thirty cameras. The cameras were installed at locations based on crime data. The system is actively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was involved in the initial and subsequent implementation process. CCTV operators do not receive any special training. Constant supervision does exist for CCTV operations. A system does not exist for handling requests for images, or for determining how long images should be saved. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. The contact person did not know if state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have not yet been used in any prosecutions for criminal behavior.

J. HONOLULU (HI) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for more than ten years and the operation includes twenty six cameras. The cameras were installed at locations based on crime data. The system is passively monitored and operates on a 24/7 basis. A written policy entitled Video Monitoring System and dated July 9, 2003 does exist for CCTV operations and includes the following elements:

- The District Commander supervises all CCTV operations
- The system will be used to address the fear of crime and enhance the quality of life
- The system may be used to address street crime and monitor suspicious activity that may lead to the commission of a crime
- The system may be used to monitor public events that attract large crowds of people
- Civilian volunteers and police officers may work in the video control center after receiving training and written instructions
- Personnel monitoring cameras will not view the screens for more than two consecutive hours
- Chain of custody procedures are outlined
- Employees observing criminal activity are required to prepare a statement using a specific department form

The community was not involved in the initial and subsequent implementation process. Special training advises employees of the technical capabilities of the software and hardware. Refresher courses are held reminding personnel of the 1st Amendment and 4th Amendment issues. Constant supervision does exist for CCTV operations. Any requests for images are forwarded to the Legal Department. The images are saved for 7 days. If an operator observes a suspicious person checking car doors, the operator would wait until the offense occurs before dispatching police. State and local laws do not apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Close supervision prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

K. LITTLE ROCK (AR) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for one year and the operation includes four cameras. The cameras were installed at locations based on crime data and neighborhood requests. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was involved in the initial and subsequent implementation process. CCTV operators do not receive any special training. Constant supervision does not exist for CCTV operations. Any requests for images will be granted upon written request. The images are saved for 7 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. State and local laws do not apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have not yet been used in any prosecutions for criminal behavior.

L. LOS ANGELES (CA) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for three years and the operation includes more than fifty cameras. The cameras were installed at locations based on crime data. The system is passively and actively monitored and operates on a 24/7 basis. A written policy entitled Hollywood Area Administrative Order No. 2 and dated October 1, 2004 does exist for CCTV operations and includes the following elements:

- Cameras will only be used to observe public spaces
- A control log will document activation and deactivation of the cameras
- Images will only be viewed in secure area
- Termination is threatened for misuse of the system
- The targeting and tracking of individuals based on race, gender, ethnicity, sexual orientation, disability or other classifications protected by law is prohibited
- Areas where a person has a reasonable expectation of privacy may not be observed
- Quarterly audits are conducted to ensure compliance with the policy

- The public is notified of camera capabilities and posts warning signs in target areas
- Regular reports are prepared for CCTV camera use
- Public input will be sought for CCTV implementation

The community was involved in both the initial and subsequent implementation process. CCTV operators receive 30 minutes of special training. Constant supervision does exist for CCTV operations. Any requests for images are forwarded to the Legal Section for evaluation. The images are saved for 7-30 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. State and local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Enforcement of the written policy prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

M. MIDDLETOWN (CT) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for six years and the operation includes more than forty cameras. The cameras were installed at locations based on crime data. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was involved in both the initial and subsequent implementation process. CCTV operators do not receive special training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the Chief for evaluation. The images are saved for 30 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

N. MIDDLETOWN (NY) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for twenty-five years and the operation includes approximately thirty cameras. The cameras were installed at locations based on crime data. The system is actively monitored and operates on a 24/7 basis. A written policy for operations entitled Public Camera Policy and Procedure and dated November 11, 2004 can be found on the agency website (http://www.middletownpolice.com/cameramain.html) and includes the following elements:

- The system does not intrude upon an individual's sphere of privacy, but rather records events occurring in public space
- A warrant must be obtained in order to secretly intercept oral communications
- The department will comply with all local, federal and case law applicable to the use of surveillance cameras in public space
- Deviation from the policy's listed principles for inappropriate reasons is strictly prohibited
- Monitoring and recording will be conducted in professional, ethical and legal manner
- Personnel using the camera system will be appropriately trained and supervised
- Violations of the policy will result in disciplinary action
- Information obtained through video monitoring and recording will be used exclusively for safety, security, and other legitimate purposes
- Information obtained through monitoring and recording will only be released in accordance with the policy
- Monitoring and recording based solely on characteristics and classifications such as race, gender, sexual orientation, national origin, etc. is prohibited
- Monitoring of public areas, swellings, and businesses is limited to uses that do not violate the reasonable expectation of privacy
- The department will maintain a copy of the policy and list of camera locations on the official web site
- Personnel assigned to system operation will be trained in the technical, legal and ethical parameters of appropriate camera use
- Personnel will provide written acknowledgement indicating that they received a copy and understand the policy
- The Chief of Police will conduct periodic audits of the CCTV camera system

- The Officer in Charge of the patrol shift will be responsible for the CCTV operation
- Any view provided by a CCTV camera shall be no greater than what is available form the public sidewalk
- Personnel will not continuously view or record people displaying affection in public areas, unless such activity is criminal in nature
- Images will be stored for a maximum of 15 days
- Storing images beyond the 15 day maximum must be authorized by the Chief of Police and may be done for evidentiary (criminal or civil), investigation of wrongdoing on the part of police or other bona fide use
- Only trained Bureau Commanders or staff authorized by the Chief of Police shall be authorized to extract video footage from the system
- Images extracted from the system will be stored in a manner that will exclude access by unauthorized personnel

The community was involved in both the initial and subsequent implementation process. CCTV operators do not receive special training. Constant supervision does not exist for CCTV operations. Any requests for images are handled in compliance with the Freedom of Information Act. The images are saved for 14 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. There are New York State laws that apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Random checks by a supervisor prevent abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

O. MINNEAPOLIS (MN) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for one year and the operation includes approximately thirty cameras. The cameras were installed at locations based on crime data. The system is both passively and actively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. CCTV operators do not receive special training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the Chief for evaluation. The images are saved

for 14 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

P. NEW YORK (NY) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for five years and the operation includes more than one hundred cameras. The cameras were installed at locations based on crime data and input from the Housing Authority. The system is actively monitored and operates on a 24/7 basis. A written policy for operations does exist but was unavailable for review. The community was not involved in the initial or subsequent implementation process. CCTV operators do not receive special training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the District Attorney for evaluation. The images are saved for 7-10 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. The contact person did not know if any state or local laws apply to CCTV operations or if private agencies wishing to utilize CCTV systems are required to register with any government agency in the jurisdiction. Strong supervision prevents abuse. The department has had complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

Q. REYNOLDSBURG SCHOOL DISTRICT (REYNOLDSBURG, OH)

The school district has been utilizing CCTV surveillance systems for three years and the operation includes more than one hundred fifty cameras. The cameras were installed at locations based on input from school staff. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial or subsequent implementation process. CCTV operators receive special training. Constant supervision does not exist for CCTV

operations. Any request for images will be granted. The images are saved for 14 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. State law does apply to CCTV operations. Private agencies are required to register with a government agency in the jurisdiction. Controlling access to the video center prevents abuse. The school district has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

R. ST. PETERSBURG, (FL) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for fifteen years and the operation includes more than fifteen cameras. The cameras were installed at locations determined by CALEA guidelines. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was not involved in the initial and subsequent implementation process. The only training available for CCTV operators is on-the-job training. Constant supervision does not exist for CCTV operations. Any requests for images are handled in accordance with the Sunshine Laws. The images are saved for 30 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have not yet been used in any prosecutions for criminal behavior.

S. TAMPA (FL) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for ten years and the operation includes more than ten cameras. The cameras were installed at locations based on crime data. The system is actively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The community was involved in the initial and subsequent implementation process. Special training is initially provided for the CCTV operators and a mandatory refresher course is scheduled yearly. Constant

supervision does exist for CCTV operations. Any requests for images are handled in accordance with the Sunshine Laws. Daily images are saved for 30 days and special events for 1 year. If an operator observes a suspicious person checking car doors, the operator would permit the offense to occur before dispatching police. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Close supervision prevents abuse. The department has received 2-3 civil right claims regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

T. TRIMET TRANSIT POLICE DEPARTMENT (PORTLAND, OR)

The department has been utilizing CCTV surveillance systems for more than fifteen years and the operation includes more than 2500 cameras. The cameras were installed at locations determined by an engineering consultant. The system is passively monitored and operates on a 24/7 basis. A written policy entitled Information Technology: CCTV Use and dated May 5, 2005, does exist for CCTV operations and includes the following elements:

- Personal use of the system is strictly prohibited
- Adjustments to aim, direction or focus, and the creation of any recorded images must be authorized by a supervisor or manager
- Use of CCTV technology is not personal or private
- Employees may only review, record, download or transmit images if included within assigned duties or as specifically directed by a supervisor or manager
- Access to CCTV technology may only be permitted to authorized users
- No outside disclosure or transmittal of CCTV is permitted without the prior authorization of a manager
- CCTV images may be used for risk identification and avoidance, claims processing, law enforcement and general safety and security purposes
- Image use for training purposes must be authorized by a manager and legal counsel
- Employees should not aim, direct or focus a CCTV camera onto property adjacent to a TriMet facility unless exigent circumstances exist and a supervisor/manager authorizes such action

- Employees may not aim, direct or focus CCTV cameras on or into businesses, homes, apartments, vehicles or any other similar private, non-public space, except to track a fleeing criminal when requested by law enforcement and authorized by a manger/supervisor
- Requests for historical data must be made to the system director
- Cameras have a "home" view and if they are moved from the that view they must be returned as promptly as possible
- Employees are not to show images to an employee involved in an incident before that involved employee files a written report describing the incident
- Employees are required to review and sign a form indicating an understanding of the agency's policies and training

The community was not involved in the initial and subsequent implementation process. CCTV operators receive special training. Constant supervision does exist for CCTV operations. Any requests for images are handled in accordance with the public records release process. The images are saved for three years. If an operator observes a suspicious person checking car doors, the operator would dispatch police to prevent the crime rather than waiting for the offense to occur. The contact person did not know if any state or local laws apply to CCTV operations or if private agencies wishing to utilize CCTV systems are required to register with any government agency in the jurisdiction. Close supervision prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior (including two homicides).

U. UNITED STATES MARSHAL'S OFFICE – TULSA, OKLAHOMA

The department has been utilizing CCTV surveillance systems for twenty years and the operation includes more than thirty cameras. The cameras were installed at locations chosen by the department. The system is actively monitored and operates on a 24/7 basis. A written policy exists for cell block operations but not for public domain surveillance. The community was not involved in the initial or subsequent implementation process. The only training available for the CCTV operators is on-the-job training. Constant supervision only occurs during normal business hours. Any requests for images are forwarded to the Chief Deputy for evaluation. The images are saved for 14 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to

occur. No state or local laws apply to Federal CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Although recorded images have not yet been used in any prosecutions for criminal behavior, they have been used in several employee discipline cases.

V. UNIVERSITY OF KANSAS – KANSAS CITY CAMPUS POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for thirty years and the operation includes more than one-hundred cameras. The cameras were installed to view points of ingress and egress on designated secure buildings. The system is passively monitored and operates on a 24/7 basis. A written policy for operations entitled Closed Circuit Television Policy can be found on the agency website (http://www.kumc.edu/police/cctvhast.html) and includes the following elements:

- The system is designed to supplement patrols of police and security officers
- Cameras provide deterrent value and greater surveillance
- Cameras are to be used to provide real time information during emergencies
- Images are maintained for at least 30 days
- Cameras may or may not be monitored on a continuous basis
- There are no "dummy" cameras in the system.

The community was not involved in the initial or subsequent implementation process. There is no special training for the department's CCTV operators. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the University's legal section for review. The images are saved for approximately 30-45 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent a crime rather than wait until the offense occurs. No state or local laws apply to CCTV operations. Private agencies wishing to utilize CCTV systems are not required to register with any government agency in the jurisdiction. Close

supervision prevents abuse. The department has not received any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

W. VIRGINIA BEACH (VA) POLICE DEPARTMENT

The department has been utilizing CCTV surveillance systems for ten years and the operation includes more than ten cameras. The cameras were installed at locations based on crime data. The system is passively monitored and operates on a 24/7 basis. A written policy for operations does not exist. The contact persons did not know if the community was involved in the initial implementation process. CCTV operators do not receive any special training. Constant supervision does not exist for CCTV operations. Any requests for images are forwarded to the Internal Affairs Bureau for evaluation. The images are saved for 60 days. If an operator observes a suspicious person checking car doors, the operator dispatches police to prevent the crime rather than waiting for the offense to occur. State and local laws do not apply to CCTV operations. The contact person did not know if private agencies wishing to utilize CCTV systems are required to register with any government agency in the jurisdiction. Controlling access to the video center prevents abuse. The department has not had any complaints from the public regarding the use of its cameras. Recorded images have been used in prosecutions for criminal behavior.

Agency	How long has agency had CCTV?	How many cameras are in the system?	How was decision made regarding placement of cameras?
Alexandria (VA) PD	18 years	>60	Security consultant
Anchorage (AK) PD	10 + years	6	Crime data based
Atlanta (GA) PD	1 year	>30	Based on funding sources
Baltimore (MD) PD	4 years	>200	Crime data based
Centennial School District (Portland, OR)	10 + years	>80	School staff input
Charlotte-Mecklenberg (NC) PD	15 years	>100	Crime data based
Chicago (IL) PD	2 ½ years	>100	Crime data based
Dallas (TX) PD	2 ½ years	>80	Crime data based
Fresno (CA) PD	<1 year	>30	Crime data based
Honolulu (HI) PD	10 + years	>20	Crime data based
Little Rock (AR) PD	1 year	4	Crime data based/neighborhood request

Table One

Agency	How long has agency had CCTV?	How many cameras are in the system?	How was decision made regarding placement of cameras?
Los Angeles (CA) PD	3 years	>50	Crime data based
Middletown (CT) PD	6 years	>40	Crime data based
Middletown (NY) PD	25 years	App 30	Crime data based
Minneapolis (MN) PD	1 year	App 30	Crime data based
New York (NY) PD	5 years	>100	Crime data based
Reynoldsburg School District (Reynoldsburg, OH)	3 years	>150	School staff input
St. Petersburg (FL) PD	15 years	>15	CALEA guidelines
Tampa (FL) PD	10 years	>10	Crime data based
TriMet Transit Police (Portland, OR)	15 + years	App 2500	Engineering consultant
University of Kansas PD (Kansas City Campus)	30 years	>100	View points of ingress and egress to secure buildings
US Marshals Service Tulsa, OK	20 years	>30	Crime data based
Virginia Beach (VA) PD	10 years	>10	Crime data based

Table One Cont'd.

Agency	Are cameras actively or passively monitored?	Are cameras operated 24/7?	Does agency have a written CCTV policy?
Alexandria (VA) PD	Actively	Yes	Unknown
Anchorage (AK) PD	Passively	Yes	No
Atlanta (GA) PD	Passively	Yes	No
Baltimore (MD) PD	Actively	Yes	No
Centennial School District (Portland, OR)	Passively	Yes	No
Charlotte-Mecklenberg (NC) PD	Actively	Yes	No
Chicago (IL) PD	Actively	Yes	Yes
Dallas (TX) PD	Passively	Yes	No
Fresno (CA) PD	Actively	Yes	No
Honolulu (HI) PD	Passively	Yes	Yes
Little Rock (AR) PD	Passively	Yes	No

Table Two

Agency	Are cameras actively or passively monitored?	Are cameras operated 24/7?	Does agency have a written CCTV policy?
Los Angeles (CA) PD	Both	Yes	Yes
Middletown (CT) PD	Passively	Yes	No
Middletown (NY) PD	Actively	Yes	Yes
Minneapolis (MN) PD	Both	Yes	No
New York (NY) PD	Actively	Yes	Yes
Reynoldsburg School District (Reynoldsburg, OH)	Passively	Yes	No
St. Petersburg (FL) PD	Passively	Yes	No
Tampa (FL) PD	Actively	Yes	No
TriMet Transit Police (Portland, OR)	Passively	Yes	No
University of Kansas PD (Kansas City Campus)	Passively	Yes	Yes
US Marshals Service Tulsa, OK	Actively	Yes	No
Virginia Beach (VA) PD	Passively	Yes	No

Table Two Cont'd.

Agency	Did community have input during implementation?	Is there special training for CCTV operators?	Is there constant supervision for CCTV operations?
Alexandria (VA) PD	No	No	No
Anchorage (AK) PD	No	No	No
Atlanta (GA) PD	No	No	No
Baltimore (MD) PD	Yes	No	No
Centennial School District (Portland, OR)	No	Yes	No
Charlotte-Mecklenberg (NC) PD	No	Yes	Yes
Chicago (IL) PD	No	Yes	No
Dallas (TX) PD	No	Training by vendor	Yes
Fresno (CA) PD	Yes	No	Yes
Honolulu (HI) PD	No	Yes	Yes
Little Rock (AR) PD	Yes	No	No

Table Three

Agency	Did community have input during implementation?	Is there special training for CCTV operators?	Is there constant supervision for CCTV operations?
Los Angeles (CA) PD	Yes	30 minutes	Yes
Middletown (CT) PD	Yes	No	No
Middletown (NY) PD	Yes	No	No
Minneapolis (MN) PD	No	No	No
New York (NY) PD	No	No	No
Reynoldsburg School District (Reynoldsburg, OH)	No	Yes	No
St. Petersburg (FL) PD	No	No	No
Tampa (FL) PD	Yes	Yes/annual refresher	Yes
TriMet Transit Police (Portland, OR)	No	Yes	Yes
University of Kansas PD (Kansas City Campus)	No	No	No
US Marshals Service Tulsa, OK	No	No	Business hours only
Virginia Beach (VA) PD	Unknown	No	No

Table Three Cont'd.

Agency	How is decision made regarding release of images?	How long are images saved?	Is system used for crime prevention or evidence gathering?
Alexandria (VA) PD	Division Chief evaluates	Unknown	Evidence
Anchorage (AK) PD	Chief evaluates	Indefinitely	Prevention
Atlanta (GA) PD	Public Affairs evaluates	90 days	Evidence
Baltimore (MD) PD	State Attorney evaluates	28 days	Prevention
Centennial School District (Portland, OR)	Written request	14 days	Prevention
Charlotte-Mecklenberg (NC) PD	Chief evaluates	3-5 days	Prevention
Chicago (IL) PD	Chief Evaluates	72 hours	Prevention
Dallas (TX) PD	FOIA process	60-90 days	Prevention
Fresno (CA) PD	Not developed yet	Not developed yet	Prevention
Honolulu (HI) PD	Legal Section evaluates	7 days	Evidence
Little Rock (AR) PD	Written request	7 days	Prevention

Table Four

Agency	How is decision made regarding release of images?	How long are images saved?	Is system used for crime prevention or evidence gathering?
Los Angeles (CA) PD	Legal Section evaluates	7-30 days	Prevention
Middletown (CT) PD	Chief evaluates	30 days	Prevention
Middletown (NY) PD	FOIA process	14 days	Prevention
Minneapolis (MN) PD	Chief evaluates	14 days	Prevention
New York (NY) PD	District Attorney evaluates	7-10 days	Prevention
Reynoldsburg School District (Reynoldsburg, OH)	All requests granted	14 days	Prevention
St. Petersburg (FL) PD	FOIA process	30 days	Prevention
Tampa (FL) PD	FOIA process	30 days/special events – 1 yr	Evidence
TriMet Transit Police (Portland, OR)	In accordance with public records release process	3 years	Prevention
University of Kansas PD (Kansas City Campus)	Legal Department evaluates	30-45 days	Prevention
US Marshals Service Tulsa, OK	Chief Deputy evaluates	14 days	Prevention
Virginia Beach (VA) PD	Processed through IA	60 days	Prevention

Table Four Cont'd.

Agency	Do any state or local laws exist regulating CCTV?	Are private CCTV operations required to register?	How is abuse prevented?
Alexandria (VA) PD	Unknown	Yes, with the state	Adherence to written policy
Anchorage (AK) PD	No	No	Controlled access to video center
Atlanta (GA) PD	No	No	Controlled access to video center and monitoring of operators
Baltimore (MD) PD	No	No – licensing for security companies	Close supervision
Centennial School District (Portland, OR)	Unknown	No	None
Charlotte-Mecklenberg (NC) PD	No	No	Limited access to system
Chicago (IL) PD	No	Unknown	Training, close supervision, controlled access
Dallas (TX) PD	No	No	Controlled access to video center
Fresno (CA) PD	Unknown	No	Controlled access to video center
Honolulu (HI) PD	No	No	Close supervision
Little Rock (AK) PD	No	No	Controlled access to video center

Table Five

Agency	Do any state or local laws exist regulating CCTV?	Are private CCTV operations required to register?	How is abuse prevented?
Los Angeles (CA) PD	No	No	Policy guidelines
Middletown (CT) PD	No	No	Controlled access to video center
Middletown (NY) PD	State law	No	Random checks by supervisor
Minneapolis (MN) PD	No	No	Controlled access to video center
New York (NY) PD	Unknown	Unknown	Close supervision
Reynoldsburg School District (Reynoldsburg, OH)	State law	Yes	Controlled access to video center
St. Petersburg (FL) PD	No	No	Controlled access to video center
Tampa (FL) PD	No	No	Close supervision
TriMet Transit Police (Portland, OR)	Unknown	Unknown	Close supervision
University of Kansas PD (Kansas City Campus)	No	No	Close supervision
US Marshals Service Tulsa, OK	No	No	Controlled access to video center
Virginia Beach (VA) PD	No	Unknown	Controlled access to video center

Table Five Cont'd.

Agency	Have any complaints been received regarding CCTV?	Have images been successfully used in prosecution?
Alexandria (VA) PD	No	No
Anchorage (AK) PD	No	No
Atlanta (GA) PD	No	Yes, more than 12
Baltimore (MD) PD	No	Yes
Centennial School District (Portland, OR)	No	Yes
Charlotte-Mecklenberg (NC) PD	No	Yes
Chicago (IL) PD	No	Yes
Dallas (TX) PD	No	No
Fresno (CA) PD	No	No
Honolulu (HI) PD	No	Yes
Little Rock (AR) PD	No	No

Table Six

Agency	Have any complaints been received regarding CCTV?	Have images been successfully used in prosecution?
Los Angeles (CA) PD	No	Yes
Middletown (CT) PD	No	Yes
Middletown (NY) PD	No	Yes
Minneapolis (MN) PD	No	Yes
New York (NY) PD	Yes	Yes
Reynoldsburg School District (Reynoldsburg, OH)	No	Yes
St. Petersburg (FL) PD	No	No
Tampa (FL) PD	Yes/2-3 civil rights claims	Yes
TriMet Transit Police (Portland, OR)	No	Yes – including 2 murders
University of Kansas PD (Kansas City Campus)	No	Yes
US Marshals Service Tulsa, OK	No	Employee discipline only
Virginia Beach (VA) PD	No	Yes

Table Six Cont'd.

V. RECOMMENDATIONS

Homeland Security professionals are utilizing public domain surveillance systems to protect critical infrastructures and institute a protective electronic net over society. Although CCTV's usefulness as a post incident investigative tool remains its most appealing characteristic, public safety professionals are eager to obtain these systems under the guise of incident prevention. Even as millions of dollars are earmarked for this technology, standardized measures and legal standards have not been implemented to prevent abuse. Actual or perceived abuse has the potential to destroy society's faith in the positive use of video surveillance systems. The research conducted for this thesis netted several methods of preventing abuse. This chapter presents step by step methods for administrators to adopt in order to maintain the fragile balance between public safety needs and privacy expectations.

A. IS CCTV THE BEST SOLUTION FOR THE PROBLEM?

When deciding whether a jurisdiction would benefit from the implementation of CCTV surveillance systems, several questions must be considered. Crucial in abuse prevention, this stage should determine if video surveillance can be effective in addressing a specifically identified problem. If a system does not have a high probability of succeeding in its stated purpose then it will face the chance of being used for unintended purposes. Those unintended purposes may involve voyeurism, racial profiling, labor rule enforcement or infringement upon the 1st and 4th Amendment rights.

A multi-discipline evaluation group should be established using representatives from the police, homeland security, emergency management, academic, legal, political, business, civic, religious, civil liberties protection, and technical field of video surveillance. The consortium should determine if introducing surveillance systems to the public domain would be the most appropriate course of action for the problem in that jurisdiction. Consideration should be directed at whether other problem solving methods would be more effective and/or more efficient. When considering possible alternatives to surveillance systems for Homeland Security issues, several possibilities should be examined. The initiation of town watch programs, improved lighting, hardening of

potential targets, integrating private security with public safety, restricting access to specific areas, and redeployment of police resources are all possible alternatives to surveillance systems tasked with protecting the public domain and critical infrastructure locations.

The group should examine research conducted on addressing the criminal or homeland security issue that has prompted the recommendation for CCTV surveillance. Studies completed in other jurisdictions may provide the group with a different perspective on solving the problem. The research may also provide valuable data to support the proposed introduction of video surveillance for the public domain. Another question that should be answered by research is whether or not the system will be able to maintain operation for an extended period of time. Sustainability has been the downfall of several system applications throughout the country. If manpower commitments or funding sources cannot be guaranteed for the project then it may be doomed before it begins.

B. CAMERA PLACEMENT

Once CCTV technology is selected as the best platform for launching an attack on a public safety threat, administrators must then decide where the cameras should be installed, as well as what areas will be observed by government authorities. The review of police systems in the United States revealed an overwhelming reliance on crime data to determine placement of surveillance cameras. Very few jurisdictions used community input, hazard analysis of critical infrastructures, or guidance from Homeland Security professionals to assist in the decision making process. By incorporating these additional viewpoints, the system can be multifaceted, gain resources from other disciplines and qualify for funding that encourages collaborative efforts.

Every city has formal and informal organizations that include business, civic, professional, educational, religious, political, and labor groups. Each of these groups should be urged to provide their input in order to assist CCTV administrators in deciding what areas require observation. This outreach by the system administrators will result in support for the program and ground level intelligence. The importance of inviting non-

law enforcement entities into the development of the program cannot be underestimated. Involvement by these groups will net huge results exhibited by fresh ideas and program buy-in.

Crime data should be reviewed longitudinally to establish historical patterns. The information should then be evaluated to ascertain whether video surveillance can assist in *preventing* future offenses. If the function of the system targets homeland security issues, crime prevention should be considered as a secondary purpose. By including crime prevention goals for the system, the presentation to convince city leaders of the system's value becomes stronger and more diverse. Additionally, utilizing the video technology to address crime issues hones the skills of the camera operators so that when a homeland security danger presents itself, the operators will be well practiced and confident in their response.

Most cities utilize their surveillance systems primarily for engaging the common street criminal. A clear need exists to factor in elements that could broaden the horizons of the technology. By blending in the goals of other disciplines focused on homeland security, system administrators can improve investigative capabilities, detect terrorist pre-planning, and thwart attacks before they occur.

Hazard analysis for critical infrastructure locations has occurred in most of America's major cities. A variety of mathematical means exist to analyze the threat to facilities that could affect services, economy and the continuity of government for the jurisdiction. If a critical infrastructure hazard analysis has not been conducted, an accepted method of prioritizing importance should be executed. The results should then be used to gauge where CCTV surveillance could best serve the public safety mission. By utilizing mapping software, authorities can visualize the hazard analysis results and avoid camera coverage duplication.

The review conducted of agencies utilizing CCTV surveillance in the United States revealed that 70% of departments used crime data as the main factor in the decision-making process regarding camera placement. Agreements with organizations

and communities funding camera costs guided 8% of the departments. Consultants assisted 8% of the departments. Critical infrastructure assessments directed 8% of the departments.

C. PUBLIC NOTIFICATION

CCTV effectiveness studies show that the deterrence effect occurs when two elements exist: 1) adequate signage and 2) swift response to suspicious behavior. Deterrence affects the criminal mindset. Minimizing secrecy and instituting adequate abuse prevention controls increases faith in government. It is imperative that public meetings be held prior to introducing CCTV technology to monitor the public domain. In the article, "Closed Circuit Television Looking Out for You," published by the British Government, CCTV administrators are advised to carefully plan and competently manage the systems to prevent actual or perceived abuse.[81] Concerns regarding civil liberties must be adequately addressed before CCTV can be successfully introduced to the public domain.

Once a decision has been made to utilize CCTV surveillance, extensive media coverage should be encouraged. City residents should understand the purpose of the system, be introduced to its manager, be aware of the steps being taken to prevent abuse, and know the procedure for filing complaints. Residents and visitors should be able to easily determine the general areas of video monitoring. Whenever the technology results in specific incidents indicating success, the examples should be publicized.

Highly visible signs should be posted on the perimeter of zones subject to video surveillance. In a survey conducted in Great Britain during 2004, the participants felt strongly that signage should alert people to ongoing CCTV surveillance. This step constitutes the deterrence element of video technology. The only way that wrongdoing can be avoided lies in the criminal element thinking that their actions will be detected, recorded, and used for prosecution.

Several jurisdictions have systems funded completely by community groups or local corporations. Since funding in Atlanta (GA) originated from the business community, the camera system focused on the commercial district. Little Rock (AR)

[81] Edwards and Tilley, "Closed Circuit Television Looking Out For You."

received its funding from neighborhood associations that enabled video surveillance of the areas represented by the donating organizations. The same applied to Los Angeles (CA) which received partial financial assistance from private entities. Municipalities permitting donations to fund CCTV surveillance systems inevitably require camera coverage of the benefactor's neighborhood. Funding partnerships should result in collaboration between community and government interests when it comes to the placement of surveillance cameras.

A careful balance must be struck between full disclosure of camera locations and maintaining operational secrecy for homeland security functions. Jurisdictions should beware of requiring all camera locations to be publicly known. There may be cause at a later time to install video surveillance tasked with observing critical infrastructure locations. Enemies should not be able to easily obtain the locations of some surveillance cameras. The answer to this conundrum may be to use citizen input to assist in prioritizing locations desirous for surveillance coverage but to maintain secrecy regarding the actual locations of the camera pods.

In Philadelphia (PA), City Councilman Darrell Clarke has responded to the debate regarding whether municipalities should have government operated CCTV surveillance systems by suggesting that the citizens decide the matter for the elected officials. He has urged that a question be placed on the ballot during the next election asking people whether they support the use of such technology for public domain monitoring. This method may be the most accurate means available to garner a true picture of whether citizens in a particular jurisdiction support the use of a potentially invasive technology in their neighborhoods.

The review conducted of agencies utilizing CCTV surveillance in the United States revealed that 65% of the departments did not seek input from the community prior to implementation of CCTV for the public domain. Several jurisdictions created community advisory groups to assist law enforcement in the introduction of this technology. One significant use of external groups as advisors occurred in the City of Los Angeles. Prior to implementation, input was sought from the American Civil Liberties Union (ACLU).

D. REGISTERING PRIVATE CAMERA SYSTEMS

The cost of implementing electronic homeland security grids protecting our nation's cities continues to be overwhelming. While local governments struggle to muster the financing necessary to install, operate and manage CCTV platforms, private entities have fully functioning systems already in use. Many of those systems observe public areas in their quest to protect private property or while monitoring the actions of the company's employees. Any system that views public areas should be required to submit to an established registration and standardization process.

Registering privately owned camera systems accomplishes two goals. The first is government's responsibility to protect the privacy expectations of society. The registration process should include a presentation to a government approved panel that would decide the merit and need for a system to observe the public in its daily routines. The presentation would answer questions such as: what will the system be used to watch, why does company management feel that this technology is the best method to address the problem, how will abuse be prevented, will the images be recorded, how long will images be saved, what will the procedure be for approving the release of images, and who will be the manager for the system. Advising private entities of the regulations established to control CCTV surveillance systems serves as the second goal of registration.

A technology approval panel should be created by the local government in order to review registration requests by private entities. The panel should determine whether the intended function of the system protects privacy expectations and meets standardization requirements. Registration renewal should be a yearly occurrence that reviews whether the system's effectiveness warrants continued operation. The process should also serve as a procedures refresher for the system administrator.

The registration process should include the geographic area that each privately operated camera spans. By providing this information, the public safety professionals will have the ability to create a map that indicates what cameras are monitoring public areas. This information can then be used in criminal and terrorism investigations. This process will also assist surveillance system administrators in deciding where to install

cameras as funding becomes available. Rather than duplicating coverage already in place, government cameras can be focused on areas that have no CCTV monitoring.

The review conducted of agencies utilizing CCTV surveillance in the United States revealed that only 8% of the jurisdictions required registration, certification or licensing for privately operated CCTV surveillance systems. Ohio requires licensing and Virginia demands certification. Maryland regulates private security companies using surveillance systems. Los Angeles (CA) plans on developing a registration process, but it is not in place at this time.

E. MECHANIZING SURVEILLANCE CAMERA OPERATION

As technology improves, software and hardware enable video surveillance that minimizes the opportunities for abuse. London's digital camera system known as the "Ring of Steel" allows counter terrorism specialists to record the license plate of every vehicle entering the city. While the system records the tag numbers of all vehicles, it also analyzes each tag using automatic number plate recognition (ANPR) software.[82] The London operation functions without the need for camera operators. Another software package can be programmed to identify special patterns of movement or entry into secure areas. Once the system identified a movement pre-designated as suspicious, a notification would be sent to a human operator who could then manually conduct an investigation using the appropriate camera.[83] Chicago (IL) has computer operated CCTV surveillance cameras that notify police when persons are identified as loitering near critical infrastructure locations, parking vehicles in restricted areas or leaving packages unattended.[84]

Disciplines other than law enforcement have introduced surveillance camera technologies that can be applied to homeland security intelligence gathering efforts. In Sacramento (CA), parking enforcement units use license plate recognition software to record every license tag that the camera observes, note its geographic position, and

[82] McCahill and Norris, "CCTV in Britain," 24.

[83] Irish Independent, "Why there's no magic shield against terror," July 16, 2005, http://www.independent.co.uk [Accessed July 2005].

[84] PoliceOne.com,"Chicago Moving to 'Smart' Surveillance Cameras," (September 22, 2004), http://www.policeone.com/policeone/frontend/parser.cfm?object=News&operation=full_news&id=92023 [Accessed July 2005].

analyze the tag. The parking authority utilizes the video equipment to determine if the vehicle has remained parked beyond the legal limit or if it is reported stolen.[85] The same data and images could be used by homeland security intelligence analysts to identify the vehicles of subjects on watch lists and other suspect modes of transportation. This information gathering mission can occur without human manipulation of the images.

Police agencies such as East Orange (NJ) and the University of Pennsylvania utilize software that automatically block out windows, fenced in yards and other specifically identified locations. These types of software remove the possibility of camera operators using the video equipment to view areas that have an expectation of privacy.

Many law enforcement systems use automatically scanning cameras that continuously record and store images. The capability exists to flag any manual override that occurs. If an operator who is expected to monitor automatically scanning or fixed cameras commands the equipment to view areas that are in conflict with the programmed system, a supervisor receives notification of the override. This permits the supervisor to view the segment of video that was generated by the operator.

F. ADMINISTRATIVE CONTROLS

Adequate controls remain the most important link between the community's faith in their government and successful implementation of CCTV surveillance systems for the public domain. People want to believe that government agents will act in a manner that protects civil liberties. If incidents occur in which trusted persons violate the social contract between government and its citizens, controversial technologies will be rejected. Administrative controls must be established to protect the citizens, program and system. The following elements can provide the foundation for controlling behavior of employees and prevent mistakes that result in organizational embarrassment.

- **Adequate supervision** – strong supervision should always be present whenever surveillance camera operations are activated
- **Specific administrator** – one management employee should be designated as the person responsible for CCTV operations and be held personally accountable for the actions of the surveillance system employees

[85] Merrill Douglas, "Parking Spotter," *Government Technology Magazine* (June 27, 2005): 68.

- **Limited access** – the video control room should be off limits to all unauthorized personnel
- **Privacy separation** – the video control room must be physically separated from all other functions to ensure privacy and protect the integrity of the operation
- **Control log** – a log should be maintained at the video control center indicating the employees and supervisors working each shift; documenting any unusual incidents; recording reasons for manual overrides of cameras; noting requests for information or copies of images; listing of all persons gaining access to the video center
- **Confidentiality agreement** – all operators should be required to sign an agreement acknowledging an understanding of the operational policies, image release standards and behavior requirements
- **Custody chain** – recorded images must be handled in a manner to prevent challenge to their authenticity; procedures should be initiated to maintain security of the DVD, hard drive or other storage format; and the number of persons handling the recorded images should be kept to a strict minimum
- **Electronic protection** – recording formats should have watermarking, encryption or some other technological method of verifying video authenticity
- **Written policy** – as with all other important programs instituted within an organization, the guidelines must be known to the employees in order to reduce liability and provide direction

The review conducted of agencies utilizing CCTV surveillance in the United States revealed that 30% of the jurisdictions activate strong on-scene supervision whenever CCTV surveillance operates. Many of the departments limit access to the video control center as a method to prevent abuse. Of the agencies surveyed, only TriMet Transit and the Middletown (NY) Police Departments require its employees to sign a confidentiality agreement restricting release of images. Shockingly, only 26% of the departments have issued a written policy detailing the guidelines to be followed while using the technology.

G. CREATION OF LEGISLATION

Legislative bodies have exhibited tremendous reluctance to create laws limiting CCTV surveillance system operations. The threat of terrorism and urban crime has generated a blind eye to the need for regulations. The average American wants Homeland Security professionals to have the authority to utilize technology in its efforts to protect society. Unfortunately, legal standards are often implemented in response to an

abuse that becomes publicized. The knee-jerk reaction can result in overzealous controls that limit the ability of well intentioned public safety professionals. The need for reasonable legislation that regulates use and protects images prevents such overreactions. By collaborating with legislators before an abuse occurs, homeland security officials can mold the legal standards to assist them in their mission and to encourage positive professional behavior.

When in-car video (ICV) became a common equipment addition for police vehicles, states instituted legal regulations regarding the length of time that images could be maintained. The Commonwealth of Pennsylvania requires that images obtained through the use of ICV be maintained no longer than 45 days from the date of recording. The exceptions to the time restrictions include evidentiary images, recordings necessary for ongoing investigations, and video utilized for training. The same restrictions established for ICV operations should be implemented for CCTV systems.

While regulations already exist for the maximum amount of time that images may be stored, consideration should be given to requiring all CCTV operations—government and private—to save images for a minimum number of days. If a surveillance system is trained on the public domain, the operation should store the images for a minimum of seven days in order to allow public safety professionals to determine if those videos can be used in their intelligence gathering and crime solving missions.

Many cities, including Chicago (IL) and Baltimore (MD), utilize video pods which are wireless cameras that transmit images via an intranet system. Since wireless systems are susceptible to interception and legislation should be drafted protecting image transfer from interference. At least one organization, the University of Texas (Austin) successfully lobbied for a statute that shields the locations of cameras from public scrutiny. Texas law states that "…specifications, operating procedures, or location of a security system used to protect public or private property from an act of terrorism or related criminal activity is confidential."[86]

The Philadelphia Parking Authority holds the distinction of being an organization that successfully convinced a state legislature to create a statute protecting video images

[86] TX Stat. Ann. Sec. 418.182 as amended by House Bill 9.

from release. Although the Authority's cameras focus on traffic enforcement, the law can serve as a model for other agencies attempting to control image releases. Strong consideration should be given to enacting legal restrictions to limit private image requests. France prohibits the release of video that could interfere with an individual's personal or financial well being.

System administrators should understand that recording of public areas will undoubtedly result in requests for images to support civil claims related to infidelity, vehicle crashes, and workman's compensation. By establishing legal guidelines, requests will be avoided for images related to civil actions. The drafting of laws should be considered to limit release of video for the following reasons:

- assist in terrorism/criminal investigations
- evidentiary in nature
- training of public safety professionals.

The review conducted of agencies utilizing CCTV surveillance in the United States revealed that legislation regulating surveillance system operations exists in only 8% of the jurisdictions where CCTV plays a part in the security mission. Legislation should be instituted prohibiting the sale, unauthorized transfer, or possession of surveillance system images not obtained in accordance with existing laws and regulations. By doing this, public safety professionals will have enforceable authority to address the ever-present temptation to sell images to the print and television tabloids. Creating criminal code violations for violating the community's trust may serve as a tremendous deterrent for persons in the position of handling surveillance system images.

H. TRAINING

CCTV surveillance technology will prompt legal challenges claiming a lack of administrative oversight, inadequate training for operators, Constitutional violations and privacy infringement. All of those issues must first be addressed with training. During the implementation phase for surveillance systems scheduled to monitor the public domain, training needs to be an integral segment of the plan.

Regulations should be established limiting the amount of time that operators can actively monitor the cameras. Studies have shown that the effectiveness of the operator

diminishes greatly after two hours of continuous monitoring. Regular personnel rotations should be implemented to ensure that operators remain alert and that the goal of the system maintained.

Operators should receive training on the technical application of the system so that they understand its capabilities and limitations. The span of the camera coverage should be understood completely by the persons responsible for monitoring so that when an incident occurs, the correct camera will be activated. Additionally, as the potential subject moves throughout the grid of coverage, the operators must understand where the cameras are located and what areas they view.

Employees and supervisors should submit to ethical awareness indoctrination so that the implications of wrongdoing are clear. The definitions of improper behavior should be outlined and understood. The existing laws of the jurisdiction should be explained along with the department's individual policies regarding CCTV operations. The training should be reinforced with a testing element that can indicate the need for further instruction and provide liability defense.

The review conducted of agencies utilizing CCTV surveillance in the United States revealed that a surprisingly low number of police departments provide training other than on-the-job for its surveillance camera operators. Only 30% of the agencies have special training sessions for the most crucial hub of the surveillance system – the human operators. The city of Tampa (FL) schedules a yearly refresher course for their camera operators. The seminar focuses on Constitutional issues and protection of individual privacy.

I. WRITTEN POLICY

Although professional organizations recommend publishing written policies addressing operational issues, only a very small segment of the surveyed departments have done so for CCTV surveillance system functions. The size of an organization often determines the likelihood of written guideline issuance. In many smaller departments, the message from the Chief filters to the line officers with little distortion or misinterpretation. Since larger departments suffer from the "whisper down the lane"

syndrome in which the sender's message frequently does not reflect what the end user receives, written policies play an important part in accurately transmitting instructions.

Regardless of the size of the organization, written policies serve as a valuable liability protection plan. The defense for civil actions lodged against public safety officials often hinge on what the employee was directed to do by her supervisors. Written policies remove the possibility of misinterpretation or the erroneous claim of a lack of direction from management. When an employee chooses to step outside the boundaries of the written guidelines, management maintains a strong position in defending itself by showing that the employee had received and understood the policy.

Disciplining employees who engage in wrongdoing cannot be minimized. In order to maintain the faith of the community in CCTV operations, government must be prepared to punish employees who act improperly. Written policies qualify as the foundation for discipline since it is impossible to reinforce the mission if employees are unaware of how that mission is to be attained.

A written policy should be drafted explaining the program's goals; the procedures to reach those goals; an explanation detailing responsibilities for the chain of command; steps to take ensuring data protection, security and release of images; and the legal guidelines regulating video surveillance systems. In order to avoid the pitfalls that confront surveillance system operators, the employees must understand the expectations of the system administrators. Written policies clearly define those expectations.

J. CCTV ADMINISTRATOR'S CHECKLIST

1. Establish CCTV Exploration Committee

- Include representatives from the police, homeland security, emergency management, academic, legal, political, business, civic, religious, civil liberties protection, technical field of video surveillance, etc.
- Is video surveillance the best method to address the problem?
- Determine if CCTV is the most effective/efficient method to address the problem?
- Evaluate whether townwatch programs, improved lighting, curfew legislation, hardening of potential targets, integration of private security with public safety, restricting access to high risk locations,

redeployment of police resources, etc. would be better at addressing the problem

- Identify other cities and agencies using CCTV and initiate contact to identify positives and negatives of those systems

2. Decide Whether Sustainability will Become an Issue

- How long will the commitment of personnel be able to be maintained?
- How long will funding be able to be maintained?
- How long will public and political support be maintained?

3. Explore Funding Possibilities

- Identify and apply for local, state and federal grants
- Solicit corporate sponsors
- Recruit organizations and community groups wishing coverage and willing to pay for equipment purchase and installation

4. Develop Collaborative Operation

- Involve utility providers, critical infrastructure locations, schools, high volume public areas, traffic control, crime suppression/detection, other city service agencies etc.

5. Involve the Community

- Consider introducing ballot question requesting permission to implement CCTV surveillance of public domain
- Hold town meetings to introduce idea and garner support
- Conduct an outreach effort to formal/informal organizations including business, civic, professional, educational, religious, political, labor etc.

6. Locations for Cameras

- Decide whether camera locations will be confidential or subject to full disclosure
- Conduct longitudinal review of crime data
- Utilize hazard analysis to identify high risk locations
- Commit to locations that provide funding
- Use consultant's input to assist in identifying the most effective locations
- Post signs notifying public in video surveillance areas

7. Develop Registration and Licensing Process for Public Domain

- Require private industry to answer the following questions:

- What will the system watch?
- Who will be the system administrator?
- Why does management feel surveillance system is necessary?
- What is the coverage area?
- What are the system capabilities?
- How will abuse be prevented?
- How long will images be retained?
- What is the image release policy?

- Establish regulations for private industry to adopt and provide to company's seeking registration and licensing
- Require yearly renewal that evaluates whether the need for surveillance still exists
- Enable spot checks by government entity
- Enable fines and system termination for violations

8. Establish Procedure for Response to Suspicious or Illegal Behavior

- Decide whether system will serve preventive or evidentiary purpose:
  - If preventive, system operators should have protocol regarding what to do for observations of suspicious or illegal behavior
  - If evidentiary, legal review should be conducted to determine if non-automated systems should follow preventive system protocols
  - If evidentiary, protocol for notifying police upon initiation of illegal behavior and method for transferring images to investigators

9. Mechanize Operations

- Consider utilizing cameras that automatically rotate
- Consider utilizing software that conducts face recognition
- Consider utilizing software that conducts license tag comparisons
- Consider utilizing software that identifies and locates gunfire
- Consider utilizing software that alerts system operators when traffic stops for extended periods of time or when items are left unattended in a public area
- Consider utilizing software that alerts system operators when movement occurs in restricted or high threat areas
- Consider utilizing software that blocks out windows, fenced-in yards, and special locations such as health clinics, etc.

10. Adequate Supervision

- Ensure that a supervisor is always on duty whenever cameras are monitored by human operators
- Restrict access to the video center and image storage location
- Establish control log that documents the names and hours of personnel working each shift; names, times and purpose of entry into the center by non-assigned personnel; requests for images; and noteworthy incidents

11. Confidentiality Agreement

- Require all personnel assigned to any element of the surveillance system operation to review and sign a confidentiality agreement
- Agreement should include a clause that the employee has received, reviewed and understands the department's written policy regarding surveillance system operations
- Agreement should include any laws specifically adopted to regulate surveillance system operations
- Agreement should include the warning that violations will result in termination and possible civil/criminal action

12. Chain of Custody for Images

- Images should have electronic protection such as, watermarking or encryption
- Images should be stored in secure location and any access to images should be recorded
- Release of images should only occur upon written request through a designated chain of command
- Release of images should be limited to:
  - assist in terrorism/criminal investigation
  - evidence indicating the commission of a crime
  - training for first responders

13. Creation of Legislation

- Engage lawmakers and guide in the establishment of legal standards for the operation of surveillance systems monitoring the public domain
- Establish legislation with penalties for violations including imprisonment and fines
- Restrict the release of images except as described above
- Develop a minimum and maximum time frame for image retention

- Prohibit the interception of image transfer from wireless, intranet or other electronic platforms
- If camera location confidentiality is determined to be necessary, establish legislation prohibiting the release of such information

14. Training

- Develop special training specifically for surveillance system operations
- Training should be provided for all levels of system operations from technical personnel to administrator
- Training should include Constitutional issues, case law, search and seizure regulations, state and local legislation, ethical considerations, and departmental policy
- Training should occur prior to assignment in surveillance system operations and yearly to reinforce the importance of acceptable behavior

15. Written Policy

- Develop a written policy that clearly defines the mission of the surveillance system
- Identify the system administrator responsible for all operational and administrative elements
- Explain the system capabilities
- Present parameters for system use, image retention and release, and access to video center and image storage location
- Note the legal and departmental restrictions for surveillance system operations

16. Publicity

- In order to develop and establish the deterrence factor of behavior control, the news media should be a partner in reporting the implementation of the system and any subsequent success stories or requests for help in identifying suspects

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Homeland Security professionals appear to be nudging toward the United Kingdom's model of public domain monitoring. As we emulate the Panopticon vision for protecting urban areas, we must do so with concern for privacy expectations and with an eye on preventing abuse. Our responsibility as protectors of society requires us to relentlessly pursue persons and organizations that threaten the safety of our citizens. The zeal directed towards completing that task cannot overshadow the need to prevent the potential for abuse.

As technology improves the ability of law enforcement to do more with less, consideration must be channeled towards ensuring we operate in a manner that protects our agency, our employees and our citizens. Forging forward with reckless abandon by providing no written direction, no supervision, no training, and no regulating legislation creates a recipe for disaster.

Staffed with intelligent and dedicated personnel, the homeland security discipline serves the nation in a manner unlike any other profession. Eager to protect the United States, these committed people adopt new methods and technologies quickly. It is unlikely that any other group of people is more intense about guaranteeing Americans their privacy while protecting them from danger. Coupled with adequate controls, video surveillance systems represent a tremendous opportunity to exponentially multiply the effectiveness of homeland security efforts in America.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Ronald J., Joseph L. Hoffman, Debra A. Livingston, and William J. Stuntz. *Criminal Procedure*. New York: Aspen Publishers, 2005.

American Bar Association Standard 2-9.1(b). "Electronic Surveillance: Technologically-Assisted Physical Surveillance." Adopted 1998.

Associated Press. "A Look at the New Orleans' CCTV System." http://www.securityinfowatch.com/article/article/jsp?id=3318&siteSection=427 [Accessed April 17, 2005].

Associated Press. "Four surveillance camera operators at N.J. casino accused of ogling female patrons." *Associated Press New York*, April 27, 2005. http://www.ap.org [Accessed August 2005].

Associated Press. "Step Up Surveillance, USA." *Wired News*, July 24, 2005. http://www.wired.com/news/privacy/0,1848,68296,00.html (Accessed December 10, 2005).

Associated Press. "Three Arrested After Traffic Camera Aimed as (sic) Passersby." *WAFF 48 News*, September 16, 2003. http://www.waff.com/Global/story/asp?S=1445080 [Accessed September 2005].

Bartol, Curt, and Anne M. Bartol. *Delinquency and Justice*. Upper Saddle River, NJ: Prentice Hall, 1998.

Bay City News. "SF cop who reportedly ogled women is suspended for 9 months." *SFGate.com*, April 21, 2005. http://www.sfgate.com/cgi-bin/article.cgi?file=/baycitynews/archive/2005/04/21/cop21.DTL [Accessed June 2005].

Beddard, Ralph. "Photographs and the Rights of the Individual." *Modern Law Review* 58, no. 6 (November 1995): 771-787.

Commission on Accreditation for Law Enforcement Agencies. CALEA Standards Manual (2005).

Cullen, Francis, and Robert Agnew. *Criminological Theory*. Los Angeles: Roxbury, 2003.

Curran, John. "Atlantic City casino fined for hidden cameras' wandering eyes." *Associated Press New York*, December 15, 2004. http://www.ap.org [Accessed December 2005].

Douglas, Merrill. "Parking Spotter." *Government Technology Magazine* (June 27, 2005): 65-72.

Edwards, Phillip, and Nick Tilley. "Closed Circuit Television Looking Out For You." *Home Office Police Research Group* (1995). http://www.homeoffice.gov.uk [Accessed April 2005].

Gargis, Jon. "Strip traffic camera zooms in on bar-goers." *University of Alabama Crimson White*, September 12, 2003. http://www.cw.ua.edu/vnews/display.v/art/2003/09/12/3f629e6e6a1fd?im_archive=1 [Accessed June 2005].

Gras, Marianne L. "The Legal Regulation of CCTV in Europe." *Surveillance & Society* (2004): 216-229. http://www.surveillance-and-society.org/articles2(2)/regulation.pdf [Accessed May 2005].

Helten, Frank, and Bernd Fischer. "What Do People Think About CCTV? Findings From a Berlin Survey." *Berlin Institute for Social Research* (February 2004): 12-18.

Irish Independent. "Why there's no magic shield against terror." July 16, 2005. http://www.independent.co.uk [Accessed July 2005].

Kinzer, Stephen. "Chicago Moving to 'Smart' Surveillance Cameras." *New York Times*, September 21, 2004, late edition, sec. A.

Koskela, Hille. "'Cam Era'-the contemporary urban Panopticon." *Surveillance & Society* (2003): 292-313. http://www.surveillance-and-society.org/articles1(3)/camera/pdf [Accessed May 2005].

Kyllo v. U.S., 121 S. Ct. 2038 (2001).

Light, Stephen. *Understanding Criminal Justice*. Belmont, CA: Wadsworth Publishing, 1999.

Livingston, Ikimulisa, and Philip Messing. "New York Police Seek Leak of Video." *Officer.com* (April 1, 2004). http://www.officer/article.jsp?id=11339&siteSection=1 [Accessed June 2005].

Marshall, Patrick. "Privacy Under Attack." *Congressional Quarterly* 11, no. 23 (June 15, 2001): 511-520.

McCahill, Michael, and Clive Norris. "CCTV in Britain." *Center for Criminology and Criminal Justice-University of Hull-United Kingdom* (March 2002): 1-70. http://www.urbaneye.net [Accessed July 2005].

Mullen, Frank X. "UNR's camera network raises fear." *Reno Gazette-Journal*, March 13, 2005, sec. 1A. http://news.rgj.com [Accessed July 2005].

New York State Governor's Press Releases. "Stephanie's Law Creates Criminal Penalties for Covert Use of Viewing Devices on Unsuspecting Victims." June 23, 2003. http://www.ny.gov/governor/press/03/june23_1_03.htm [Accessed June 2005].

New York Civil Liberties Union. "Surveillance Camera Project." http://www.nyclu.org/surveillance_camera_main.html (Accessed December 10, 2005).

Ney, Steven, and Kurt Pichler. "Video Surveillance in Austria." *Urbaneye Project* (April 2002). http://www.urbaneye.net [Accessed July 2005].

Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Wear Simmons. "Public and Private Applications of Video Surveillance and Biometric Technologies." *California Research Bureau* (CRB 02-006 2002): 1-67. http://www.library.ca.gov/CRB/02/06/02-006.pdf [Accessed August 2005].

Nieto, Marcus. "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" *California Research Bureau* (1997): 1-45. http://www.library.ca.gov/CRB/97/05/crb97-005.pdf [Accessed August 2005].

Parliamentary Office of Science and Technology. "CCTV." *Postnote* no. 175 (April 2002): 1-4. http://www.parliament.uk/post/pn175.pdf [Accessed June 2005].

PoliceOne.com. "Chicago Moving to 'Smart' Surveillance Cameras." (September 22, 2004). http://www.policeone/policeone/frontend/parser.cfm?object=News&operation=fullnews&id=92023 [Accessed July 2005].

Reid, Tim. "US surveillance will track every car." *Times* (London), July 3, 2003. http://www.globalsecurity.org/org/news/2003/030703-car-surveillance01.htm [Accessed August 2005].

Ruegg, Jean, Valerie November, and Francisco Klauser. "CCTV, Risk Management and Regulation Mechanisms in Publicly-Used Places: A Discussion Based on Swiss Examples." *Surveillance & Society* (2004): 415-429. http://www.surveillance-and-society.org/cctv.htm [Accessed May 2005].

Saetnan, Ann Rudinow, Johanne Yttri Dahl, and Heidi Mork Lomell. "Views from under surveillance. Public opinion in a closely watched area in Oslo." *Urbaneye Project* (January 2004). http://www.urbaneye.net [Accessed May 2005].

Sheptycki, James. "Surveillance, Closed Circuit Television and Social Control." *Policing and Society* 9 (2000): 430-436.

Sonner, Scott. "Nevada researcher alleges university police falsely reported homeland security concerns." *Associated Press New York*, April 23, 2005. http://www.ap.org [Accessed July 2005].

Stearns, John. "2 at casino fired for breast photos dealers, customers pictured." *Arizona Republic*, June 5, 2004, sec. B1. http://www.azcentral.com/news/ [Accessed August 2005].

Surveillance Camera Players. "Maps of Publicly Installed Surveillance Cameras in New York City." http://www.notbored.org/scp-maps.html [Accessed December 10, 2005].

Surveillance Camera Players. "Who we are & why we're here." http://www.notbored.org/generic.ipg [Accessed December 10, 2005].

Topfer, Eric, Leon Hampel and Heather Cameron. "Watching the Bear." *Urbaneye Project* (December 2003). http://www.urbaneye.net [Accessed July 2005].

TX Stat. Ann. Sec. 418.182 as amended by House Bill 9.

Wallace, Sarah. “NYPD Housing Surveillance Staffed by Cops Under Investigation.” *Officer.com* (April 23, 2004). http://www.officer.com/article/article.jsp?id=1207&siteSection=1 [Accessed August 2005].

Wardle, Amanda. “Company denies charges.” *Nashville City Paper*, August 1, 2003 http://www.nashvillecitypaper.com/index.cfm?section_id=9&screen=news&news_id=25248 [Accessed December 10, 2005].

Welsh, Brandon C., and David P. Farrington. “Effects of Closed Circuit Television Surveillance on Crime: Protocol for a Systematic Review.” *Campbell Collaboration Crime and Justice Group* (2003): 1-12. http://www.campbellcollaboration.org/doc-pdf/cctv.pdf [Accessed June 2005].

Wiecek, Carsten, and Ann Rudinow Saetnan. “Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark.” *Urbaneye Project* (March 2002). http://www.urbaneye.net [Accessed July 2005].

Williams, Katherine, and Craig Johnstone. “The Politics of the Selective Gaze: Closed Circuit Television and the Policing of Public Space.” *Crime, Law & Social Change* (September 2000): 183-210.

Wilson, Dean, and Dr. Adam Sutton. “Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation.” *A Report to the Criminology Research Council* (November 2003): 1-6.

Woodward, John D. “Privacy vs. Security: Electronic Surveillance in the Nation’s Capital.” *RAND Corporation* (CT-194 2002): 1-11. http://www.rand.org/pubs/testimonies/ct194/index.html [Accessed August 2005].

Zurawski, Nils. “I Know Where You Live!-Aspects of Watching, Surveillance and Social Control in a Conflict Zone.” *Surveillance & Society* (2005): 498-512. http://www.surveillance-and-society.org/articles2(4)/ni.pdf [Accessed September 2005].

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California